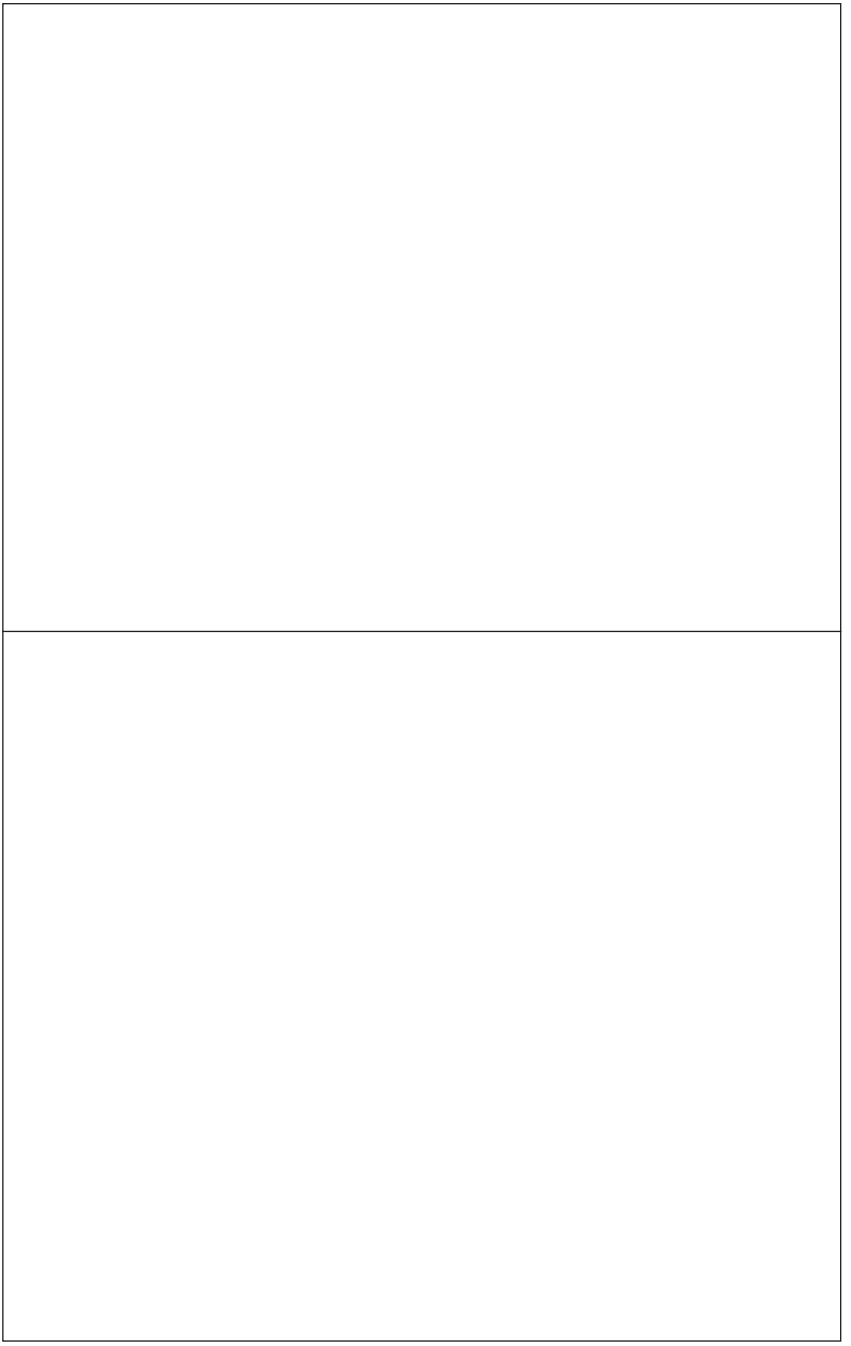
Camilla Crea | Alberto De Franceschi (Eds.)

The New Shapes of Digital Vulnerability in European Private Law

Nomos



Camilla Crea | Alberto De Franceschi (Eds.)

The New Shapes of Digital Vulnerability in European Private Law

Prefaces by
Frank Pasquale and Oreste Pollicino

Nomos

This volume is funded by the Italian Ministry of University and Research as a 'Research Project of National Interest (PRIN) 2020XBFME2'

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

1st Edition 2024

Published by
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Production of the printed version:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-1632-7 (Print)
ISBN 978-3-7489-4091-3 (ePDF)
DOI https://doi.org/10.5771/9783748940913

Online Version
Nomos eLibrary

Table of Contents

Authors' profiles 9

Camilla Crea, Alberto De Franceschi
'Digital Vulnerability in European Private Law' – Towards Digital Fairness 17

PREFACES

Frank Pasquale
Enforcing and Expanding Legal Protections for Vulnerable Subjects 21

Oreste Pollicino
Vulnerability in the Digital Age 25

PART I Digital Vulnerability as a Paradigm for Consumer Law

Catalina Goanta, Giovanni de Gregorio, Jerry Spanakis
Consumer Protection and Digital Vulnerability: Common and Diverging Paths 31

Fabrizio Esposito
Investigating Digital Vulnerability with Theories of Harms: A Methodological Proposal with Three Illustrations 53

Emilia Mišćenić
Information, Transparency and Fairness for Consumers in the Digital Environment 89

Mateja Durovic, Eleni Kaprou
The New Concept of Digital Vulnerability and the European Rules on Unfair Commercial Practices 127

Niti Chatterjee, Gianclaudio Malgieri
The Metaverse and Consumers' Vulnerabilities 145

Shabahang Arian
Vulnerability in the Age of Metaverse and Protection of the Rights of Users Under EU Law 169

PART II Conceptualizing Digital Vulnerability Beyond Consumer Law

Mateusz Grochowski
Digital Vulnerability in a Post-Consumer Society. Subverting Paradigms? 201

Irina Domurath
Digital Vulnerability as a Power Relation: Hyper- and Hypo-Autonomy and Why Thick Privacy Matters 227

Teresa Rodríguez de las Heras Ballell
Digital Vulnerability and the Formulation of Harmonised Rules for Algorithmic Contracts: A Two-Sided Interplay 259

Jura Golub
Digital Vulnerability of Consumers in the World of Smart Contracts – Is European Private International Law "Digitalised" Enough? 293

Gérardine Goh Escolar
Addressing Digital Vulnerability Through Private International Law 325

Federica Casarosa, Hans-W. Micklitz
Addressing Vulnerabilities in Online Dispute Resolution 351

PART III Contexts and Images of Digital Vulnerable Subjects

Piotr Tereszkiewicz, Katarzyna Południak-Gierz, Patryk Walczak
The Digital Vulnerability of Insurance Consumers and Personalised Pricing of Insurance Products 383

Alessandra Pera, Sara Rigazio
Let the Children Play. Smart Toys and Child Vulnerability 413

Denise Amram
Standards to Face Children and Patients Digital Vulnerabilities 439

Isabelle Wildhaber, Isabel Laura Ebert
From Digital Vulnerability to Data Anxiety: The Situation of Employees in Digitally Permeated Workplaces 469

Léa Stiefel, Alain Sandoz
Design for Agency *vs.* Vulnerability by Design – The Case of Swiss Agriculture 499

CONCLUSIONS

Reiner Schulze
Digital Vulnerability in European Private Law – Conclusions 521

Authors' profiles

Denise Amram is a senior Assistant Professor of Comparative Private Law at LIDER Lab – DIRPOLIS Institute L'EMbeDS Department of Excellence at Scuola Superiore Sant'Anna of Pisa (Italy). At LIDER Lab, she coordinates the research lines ETHOS (EThics and law witH and fOr reSearch), Children's Rights, and the Permanent Observatory on Personal Injury Damages. Her research interests include fundamental rights enhancement and protection of vulnerable subjects in different context, especially within the digital dimension.

Shabahang Arian holds a PhD in Law from the Dirpolis Institute of the Scuola Superiore Sant'Anna in Pisa. She is currently an adjunct professor and researcher at University of Tehran where she is dedicated to advancing legal education and fostering innovative research in the field of Law and Technology.

Federica Casarosa is a Research Associate at the Scuola Superiore Sant'Anna (Pisa) and part-time professor at the European University Institute. Since her degree in Private Law (University of Pisa, 2001) and her subsequent PhD in Law (European University Institute, 2008), Federica Casarosa has directed her interests towards the intersection of law and technology, analysing the role of information in consumer contracting, the protection of consumer data and internet users, private regulation in the protection of freedom of expression, and the impact of cybersecurity legislation in private law. She has carried out both teaching and research activities on these topics.

Niti Chatterjee is a seasoned commercial and technology lawyer with over a decade of experience advising multinational corporations. Holding an advanced LLM in Digital Technology Law from Leiden University, Niti specializes in the intersection of law and technology, focusing on ethical practices in the digital realm. Currently based in Luxembourg, she is passionate about promoting the responsible use of technology and advocating for regulatory frameworks that ensure fairness and accountability in the digital landscape.

Camilla Crea is Associate Professor of Private Law at the University of Sannio. She is the founder and Editor-in-Chief of The Italian Law Journal, and serves on the editorial boards of several Italian legal journals and book series. She is the author of monographs and essays on contract law, intellectual property and private law theory, analyzed through historical, comparative and critical perspectives. She has held research and teaching positions at many foreign universities, including the University of Berkeley; Beijing Normal University; Sorbonne Université; Université Cadi Ayyad-Marrakech; Edinburgh Centre for Private Law; Florida International University; Université Paris

Nanterre; Université Catholique de Lille; and the École des hautes études en sciences sociales (EHESS).

Alberto De Franceschi is Professor of Private Law, Digital Law and International Trade Law at the University of Ferrara, Ambassador's Chair at the KU Leuven and Distinguished Visiting Professor at the UC Los Angeles. From 2021 to 2023 he was Visiting Professor at the Zhejiang University, Hangzhou. Since 2016 he has been serving as Italian Expert at EU Council, G7 Digital&Technology, UNCITRAL E-Commerce Working Group, Unidroit and the Hague Conference on Private International Law. He is co-editor of the "Journal of European Consumer and Market Law" and of "The Italian Law Journal". He is an Ordinary Member of the Academia Europaea and of the European Academy of Sciences and Art. His research deals with Law of obligations and contracts, with focus on digital economy and sustainability.

Giovanni De Gregorio is the PLMJ Chair in Law and Technology at Católica Global School of Law and Católica Lisbon School of Law. He is also a member of the Católica Research Centre for the Future of Law. His research interests include digital constitutionalism, fundamental rights, technologies and digital policy. Giovanni is the author of the monograph Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society (Cambridge University Press 2022).

Irina Domurath is Adjunct Professor of Law at the University Adolfo Ibañez in Santiago de Chile. Previously, she held positions at the Central University of Chile, the University of Amsterdam, and the University of Copenhagen. She researches the effects of market regulation on horizontal relationships, with case studies concerning consumer credit, access to housing, and data protection.

Mateja Durovic is Professor of Law and Co-Director of the Centre for Technology, Ethics, Law and Society (TELOS) at King's College London, where he first worked as lecturer and then as a reader in law. Previous to this, he was an Assistant Professor (2015-2017) at the School of Law, City University of Hong Kong. Dr. Mateja Durovic holds a PhD and LLM degrees from the European University Institute, Italy, LLM degree from the University of Cambridge, UK, and LLB degree from the University of Belgrade, Serbia. Dr. Durovic was a Post-Doc Research Associate at the EUI, Italy (2014-2015), Visiting Scholar at Stanford Law School, USA (2011), and at the Max Planck Institute of Private International and Comparative Law, Hamburg, Germany (2010). Dr. Durovic worked for the Legal Service of the European Commission, as well as a consultant for the European Commission, World Bank, GIZ, BEUC and the United Nations. The work of Dr. Durovic was published in leading law journals and by most prominent publishers. He is a member of the European Law Institute, Society of Legal Scholars and Society for European Contract Law.

Isabel Laura Ebert is a Senior Research Fellow at the Institute for Business Ethics and Institute for Work and Employment Research, University of St. Gallen, and serves as a Strategic Adviser to the United Nations Office of the High Commissioner for Human Rights B-Tech Project, focusing on Business & Human Rights in the technology

sector. Her research explores regulatory and policy responses to emerging human rights challenges connected with technology company conduct and implications for policy coherence. Isabel received a PhD in Business Ethics from the University of St. Gallen.

Fabrizio Esposito is a Bocconi and EUI alumnus and Associate Professor of Private at the NOVA School of Law (Lisbon). His 40+ publications combine doctrinal analysis, especially of EU consumer and regulatory law, with economics and other disciplines. His monograph, *The Consumer Welfare Hypothesis in Law and Economics,* opens a new path in 'law and economics'. He has co-edited three volumes, including the forthcoming *Cambridge Handbook on Algorithmic Price Personalization and the Law.* Fabrizio sits on the Consulting Board of the *European Review of Contract Law* and acts as class representative in two class actions against Big Tech companies.

Catalina Goanta is Associate Professor in Private Law and Technology and Principal Investigator of the ERC Starting Grant HUMANads, focused on understanding the impact of content monetization on social media and on reinterpreting private law fairness in the context of platform governance. Between 2016-2021 she was Assistant Professor at the Faculty of Law at Maastricht University, and during February 2018 - February 2019, she was a Niels Stensen fellow and visited the University of St. Gallen (The Institute of Work and Employment) and Harvard University (The Berkman Center for Internet and Society). She is also a non-residential fellow of the Stanford Transatlantic Technology Law Forum.

Gérardine Goh Escolar is Deputy Secretary General of the Hague Conference on Private International Law (HCCH), and Head of its International Commercial, Digital and Financial Law Division. Dr Goh Escolar is Full Professor (Adjunct) and Academic Fellow at the Centre for Technology, Robotics, Artificial Intelligence and the Law (TRAIL) at the Faculty of Law of the National University of Singapore.

Jura Golub, LLM, is a Research Assistant at the Faculty of Law Osijek, Croatia, and a PhD Candidate under the Croatian Science Foundation's program "Young Researchers' Career Development Project – Training of New Doctoral Students." He teaches seminar classes in Private International Law at the Faculty of Law Osijek. His research focuses on the digitalization of law, particularly on issues related to digital assets from both substantive and conflict-of-law perspectives. Jura has presented at several international scientific conferences, including those at Radboud University, the University of Milan, the University of Ferrara, the National University of Singapore, and Royal Holloway, University of London. As a recipient of a British Scholarship Trust award, he completed a two-month research stay at Kingßs College London, The Dickson Poon School of Law. He is also the author of several scientific and professional papers.

Mateusz Grochowski is an Associate Professor of Law at Tulane University School of Law and an Affiliated Fellow at the Information Society Project at Yale Law School. His research focuses on the intersections of digital market and contract law theory, the protection of weaker market participants, and the comparative study of US-EU consumer protection and regulation of digital markets. He is a member of the editorial boards of

the "Rabel Journal of Comparative and International Private Law" and the "Journal of European Consumer and Market Law", as well as a member of the consulting board for the "European Review of Contract Law".

Eleni Kaprou is a senior lecturer in Business Law in Queen Mary University of London since 2022. Prior to that she held posts in Brunel University and Cardiff. Eleni has also served as a consultant on EU projects and taught on executive programmes for civil servants. Eleni's research interests lay in European private law with a focus on vulnerable subjects. She has written on consumer vulnerability, aggressive practices and retail financial services among others. Currently she is working on aggressive practices in the digital environment.

Gianclaudio Malgieri is an Associate Professor of Law & Technology at Leiden University (the Netherlands) and a board member of the eLaw Center for Law and Digital Technologies. He serves as the Co-Director of the Brussels Privacy Hub, an Associate Editor of Computer Law and Security Review, and the founder of "VULNERA", the International Observatory of Vulnerable People in Data Protection. He conducts research on and teaches Data Protection Law, AI regulation, Fundamental Rights in the Digital Age, Legal Vulnerability. He is the author of "Vulnerability and Data Protection Law" (Oxford University Press, 2023). Gianclaudio has authored over 70 publications, including articles in leading international academic journals. His works have been cited by, inter alia, top international newspapers (The New York Times, The Washington Post, Le Monde, Politico, La Tribune, France Culture, ilSole24Ore, la Repubblica, il Corriere della Sera, Euractiv).

Hans-W. Micklitz is Part-time Professor of Economic Law, European University Institute, Florence Italy, fullt-time between 2007 and 2019, formerly Professor at the Berlin School of Business and the University of Bamberg (Germany), visiting scholar at the universities of Bologna (Italy), Columbia (USA), Florence (Italy), Helsinki (Finland), Michigan (USA) and Oxford (UK), ERC Grant 2011-2016 on European Regulatory Private Law, Grant Academy of Finland, 2017-2022 on External Dimension of European Private Law, research on European and transnational private law, compulaw, legal theory.

Emilia Mišćenić, Dr. iur. (KFU Graz), LL.M. (Saarland) is a full professor at the Faculty of Law, University of Rijeka. For her academic work in the field of European private law and consumer protection, she has been awarded by the Croatian National Science Award, the Award of the University of Rijeka Foundation, the Award of the Republic of Croatia Ivan Filipović and many others. Her work has contributed to AG's legal opinions in cases such as Pereničová and Perenič, Meta Platforms Ireland and UFC, Que choisir and CLCV AG. She is a co-chair of the award-winning European Law Institute Croatian Hub, and a head of the University of Rijeka project "Transparency and Fairness in the Digital Environment" (uniri-iskusni-drustv-23-101).

Frank Pasquale is Professor of Law at Cornell Law School and Cornell Tech. He is an expert on the law of artificial intelligence (AI), algorithms, and machine learning. His

books include The Black Box Society (Harvard University Press, 2015) and New Laws of Robotics (Harvard University Press, 2020). His work has been translated into over a dozen languages. His present research is focused on affective computing, the political economy of automation, and AI in the public sphere.

Alessandra Pera is PhD in Comparative Law and Full Professor at Palermo University-Department of Political Science and International Relations. Her research focuses on family law, ADR systems and protection of vulnerable individuals and groups. Member of the International Society of Family Law (ISFL), the Italian Association of Comparative Law (AIDC) and Juris Diversitas. She has been visiting at the IALS University of London, the Cape Town University, the Rey Juan Carlos University of Madrid, the Hanu-Hanoi University. Member of the Editorial board of Comparazione e Diritto Civile, Comparative Law Review, International Journal of Law and Society, Cardozo Electronic Law Bulletin.

Oreste Pollicino is Professor of Constitutional Law at Bocconi University. His research interests focus on European and Comparative Constitutional Law, and Digital Constitutional Law. He is the Director of the LLM in Law of Internet Technologies at Bocconi University. He has been appointed by the European Commission for the negotiation on the 'European code of practice on disinformation'. He is also member of the Executive Board, European Union Agency for Fundamental Rights, and of the European Commission Sounding Board of the Multistakeholder in the fight against online disinformation. He is participant to the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), and Italian member of the OECD Global Partnership on Artificial Intelligence.

Sara Rigazio is PhD in Private Law, holds a LL.M. from the University of Minnesota Law School and is Assistant Professor of Private Law at the department of Political Sciences and International Relations at the University of Palermo. She has been visiting fellow at the Norwegian Center for Computer and Law at the University of Oslo. She has published several articles and a book on family law, national and international child protection, legal design and the relationship with new technologies.

Katarzyna Południak-Gierz Ph.D. (Jagiellonian University in Kraków) is a senior lecturer at the Jagiellonian University's Private Law Department. Her academic interests focus on the interplay between private law and technology. She researches private law reactions towards the use of personalization techniques in consumer contracts and the possibility of using granularity to increase the ecological efficiency of sales law.

Teresa Rodríguez de las Heras Ballell is Full Professor of Commercial Law at University Carlos III of Madrid, Spain. She was Sir Roy Goode Scholar at Unidroit 2021–22. She is the Delegate of Spain at UNCITRAL for WGs VI, IV (on AI in international trade) and I, and an Expert for UNCITRAL and Unidroit on digital economy projects. Arbitrator. Member of the Austrian Academy of Sciences. Member of the European Commission Expert Groups on Liability and New Technologies, for the Observatory

on Online Platform Economy, and on B2B Data Sharing. Member of the ELI Executive Committee and Council, and co-reporter of ELI Algorithmic Contracting Project.

Alain Sandoz holds a MSc in mathematics from Neuchâtel University and a PhD in computer science and distributed information systems engineering from EPFL, Lausanne. His interests are related to distributed information systems design and implementation; the role of scale and complexity in innovation strategy; and information infrastructures. He is lecturer and professor at Neuchâtel University and has been teaching informatics and strategy at higher education institutions in Switzerland since 1995.

Reiner Schulze is Professor Emeritus of German and European Civil Law and Director of the Centre for European Private Law at the University of Münster, Germany. He is a founding member of the European Research Group on Existing EC Private Law and the European Law Institute, as well as foreign member of the Italian Accademia Nazionale dei Lincei and the Spanish Real Academia de Jurisprudencia y Legislación. He has published extensively in the field of European private law, contract and consumer law, and digital law with books including *European Contract Law* (3rd edn, co-written with Fryderyk Zoll), *EU Digital Law* (2nd edn, co-editor with Dirk Staudenmayer), and *Bürgerliches Gesetzbuch Handkommentar* (12th edn).

Gerasimos (Jerry) Spanakis is an assistant professor in machine learning and data mining at Maastricht University. His current work lies in the area of Social Computing and includes computational social media modeling, dialogue systems (conversational agents) and information retrieval. More specifically, he is interested into using Large Language Models (like chatGPT) in a controlled way and build useful applications that have added value for all relevant stakeholders, especially for the legal domain. He is the PI for the VOXReality H2020 project, co-organizes the Natural Legal Language Workshop, and serves as a senior expert for the European Commission's e-enforcement academy project.

Léa Stiefel holds a PhD in Social Sciences in the field of STS and Digital Studies. Her thesis, defended and awarded at the University of Lausanne in 2023, focused on the Politics of digital architectures. She currently works as a research fellow at the Swiss Competency Centre for Penal Sanctions (cscsp.ch) in Fribourg and is also vice-president of IRIN (irin.ch), an independent research institute on digitisation based in Bulle.

Piotr Tereszkiewicz Ph.D. (Jagiellonian University in Kraków), M.Jur (Oxford), is a professor at the Jagiellonian's University Private Law Department, an adjunct professor at Cornell Law School and a senior affiliated researcher at the University of Leuven (KU Leuven). His research interests include private law, law and economics, insurance law and financial services in a comparative and international perspective. He was

Deputy Chair of the Scientific Advisory Committee at the Financial Ombudsman in Poland (2019–2021).

Patryk Walczak is a a PhD Candidate at the Jagiellonian University in Kraków, Poland.

Isabelle Wildhaber, LL.M. (Harvard Law School), is a Full Professor for Private and Business Law at the University of St. Gallen and the Executive Director at the Institute for Work and Employment Research (FAA-HSG) at the University of St. Gallen in Switzerland. Isabelle Wildhaber is admitted to the Bar in Switzerland and to the Bar in New York First Department, having previously worked for Swiss and American law firms in Basel, New York and Frankfurt a.M.

'Digital Vulnerability in European Private Law' – Towards Digital Fairness

Camilla Crea, Alberto De Franceschi

Vulnerability has emerged in legal discourse, in dialogue with other disciplines, as a useful concept to capture the fluid and multilayered nature of the human condition and to question the adequacy of some foundational legal and policy norms.

Yet, despite the potential of the notion of vulnerability as a key tool to overcome the limits of legal formalism and paternalism and to foster substantive equality, the legal status and effects of the notion under domestic and European laws are still quite unclear. Moreover, the notion of vulnerability has only seldom been applied to the specific forms of exposure to harm that might arise from interaction with digital technologies. In our current and pervasively digitalized world, it is however necessary to analyze how digital technologies impact preexisting forms of vulnerability or create new ones, and to understand how the law can prevent or address unequal experiences of technology. The current situation calls for legal perspectives and responses actively implementing humanist values and vulnerability-driven solutions.

This is what the Research Project on 'Digital Vulnerability in European Private law' (DiVE), funded by the Italian Ministry of University and Research as a 'Research Project of National Interest',[1] aims to do. In particular, the Project seeks to investigate the notion of digital vulnerability, by exploring how it stands vis-à-vis traditional paradigms of protection of weaker parties (such as rules on incapacity, consumer protection, data protection, anti-discrimination and equality before the law) and to what extent it might properly capture harms stemming from digital technologies.

Furthermore, the Project aims to test to what extent current rules adequately deal with personal conditions in which digital technology might prove particularly disruptive and challenging for the persons involved, and to assess how national and European legal principles, rules and policies could be aligned, reimagined and shaped in order to properly translate the

1 Progetto di Ricerca di Interesse Nazionale (PRIN) - Project 2020XBFME2.

notion of digital vulnerability into justiciable issues, that is, into claims for special legal protection. The European legal framework is notably seeking to act as a standard setter in the digital economy, trying to address a great number of Private Law aspects affected by technology (e.g., Privacy, Contract and Tort Law).

Therefore, this volume represents the first step within an ongoing research project that seeks: to give a more concrete meaning to the necessarily fluid concept of digital vulnerability and to clarify how the notion might be applied both on a descriptive and prescriptive level; to identify personal and situational factors that are most often linked to a condition of digital vulnerability and to provide assessment tools for diagnosing, preventing and addressing situations of digital vulnerability; to identify effective measures/remedies to ensure the utmost protection of those who may be digitally vulnerable against emerging technological threats; to help transformatively reconsider traditional private law micro- and macro-categories revolving around the notion of digital vulnerability, challenging traditional legal taxonomies.

This volume collects the papers presented and discussed at the opening conference of the project, which took place at the University of Ferrara on 15 and 16 June 2023, where the authors of the contributions exchanged their thoughts.

We would like to express our warm thanks to Frank Pasquale and Oreste Pollicino for their inspirational and detailed prefaces, as well as to Reiner Schulze for his brilliant conclusions.

Our gratitude also goes to all the distinguished Authors for their enthusiastic and valuable contributions to this volume, and to the members of the 'Digital Vulnerability in European Private law' (DiVE) project, including, further to the two editors of this volume, Marta Infantino (Principal investigator, University of Trieste), Claudia Amodio (University of Ferrara), Amalia Diurni (University of Rome Tor Vergata), Luca Ettore Perriello (Polytechnic University of Marche) and Loredana Tullio (University of Molise) for the inspiring cooperation.

Camilla Crea & Alberto De Franceschi

PREFACES

Enforcing and Expanding Legal Protections for Vulnerable Subjects

Frank Pasquale

Technological advance is almost always a double-edged sword. The same AI that can propose different chemical compounds for medicinal purposes can also suggest new poisons. Advertising targeting software may be immensely useful, but may also take advantage of vulnerabilities (by, for example, marketing cosmetics to a person when it calculates they are feeling most unattractive). Generative AI creates an enormous range of useful images, but also dramatically reduces the cost of disinformation.

Is there a way to encourage the positive side of digital advance, while curbing its negative effects? If so, law is among the most important tools for achieving this end. In *The New Shapes of Digital Vulnerability in European Private Law*, Camilla Crea and Alberto De Franceschi have assembled a remarkable set of authors to chart the path forward. The authors in this volume both propose expanded enforcement of extant law, and postulate important new protections. While I cannot convey the breadth of their contributions in a brief preface, I describe below a set of perspectives in the volume that illustrate one particular achievement of this collection – its simultaneously solid grounding in present controversies and ambitious aspirations toward a better future.

Emilia Mišćenić has starkly laid out the stakes of the present inquiry in her chapter, *Information, Transparency and Fairness for Consumers in the Digital Environment.* As she observes, "Despite the existing legal framework, businesses are only purportedly complying with legal rules. More often than not, they are circumventing or ignoring the requirements of EU consumer law related to mandatory information duties and transparency." This is an important diagnosis, justifying further inquiry into both improved enforcement and reform of present legal authorities.

In terms of law reform, Mateja Durovic and Eleni Kaprou recognize that "digital asymmetry captures the position of imbalance between traders and consumers online, alongside the embedded vulnerability of consumers." They argue in *The New Concept of Digital Vulnerability and the European Rules on Unfair Commercial Practices* that "more holistic and extensive

reform of the [Unfair Commercial Practices Directive] will be required to thoroughly adapt consumer law regulations to the fluctuating digital economy." This is an important level-setting, establishing the stakes of vulnerability-related legislation and the importance of advancing it.

Federica Casarosa and Hans-W. Micklitz expertly state the case for caution with respect to online dispute resolution systems, especially with respect to the disabled and impoverished. Their chapter *Addressing Vulnerabilities in Online Dispute Resolution* recognizes both the uses and shortcomings of digital literacy approaches. They articulate three dimensions of digital asymmetry which must be at the core of future legislation and enforcement in the area. First there is relational asymmetry, "due to the position [consumers] have in a complex digital environment where equal interaction is made impossible." The old problem of "one-shot" versus "repeat players," noted in Marc Galanter's *Why the Haves Come Out Ahead*, is profoundly exacerbated in massive platforms which are older than a fair number of their users—and more powerful than nearly all of them. Second, there is architectural asymmetry, which is only belatedly and partially addressed by restrictions on dark patterns and similar forms of manipulation via interface. Third, they analyse the problem of knowledge-based asymmetry, where "the trader benefits from detailed insights about the consumer while the consumer often knows - or understands - very little about how the trader and the service operate." Large platfoms may base their calculations on billions of transactions, while consumers have far less information—and, in concentrated commercial environments, few "exit" options to alternative providers.

Recognizing this knowledge-based asymmetry, Irina Domurath's philosophically sophisticated chapter articulates the importance of privacy to help level the informational playing field. Many forms of manipulation are based on intimate knowledge of a consumer or worker. Privacy law is not simply about informational self-governance, but also helps reduce the ability of other entities to erode the data subject's autonomy. Domurath proposes "that the concept of digital vulnerability could be stronger if it were to conceptualize the idea of privacy as the very foundation for any human action (including consumer choice)." This is a thought-provoking challenge to surveillance capitalism, logically extending Shoshana Zuboff's critique of behaviorism by deeply considering the foundations of the philosophy of action. Real human action (or human agency, in Charles Taylor's framing), rather than mere conditioned response, is premised on free

will, which is in turn dependent on some Goffman-ian "off-stage" space to reflect and plan free of any entity's prying eyes or sensors.

To be sure, critics of liberal individualism might characterize such a space as a fantasy. As Hans-Georg Gadamer recognized, we are always already socially formed in our aspirations and ideals. Nevertheless, we should also recognize that, as Jordan Stein has argued, a fantasy "picks us up and dusts us off and allows us to say to ourselves…I am not (or, as the case may be, I am) that kind of person, this action is not (or, again, is) part of the pattern, often called a personality, that adds up to me as the person I recognize myself to be."[1] The fantasy of self-governance beyond the scope of market imperatives may operate as an ever-receding, and yet still hope-inspiring, horizon of vulnerability studies. Certainly no one can blame today's oft-manipulated consumers for chasing such a dream, however often the grim realities of online commerce dash its realization.

Fabrizio Esposito's conception of "hyper-engaging" practices as particularly manipulative nudges (in his chapter *Investigating Digital Vulnerability with Theories of Harms*) illuminates the stakes of such aspirations in a particularly perceptive manner. The work of thinkers ranging from Jonathan Haidt (*The Anxious Generation)* to Lauren Berlant (particularly with respect to their theory of "cruel optimism") should motivate sophisticated commentators to reconsider liberal scholars' almost blanket rejection of critical theories of false consciousness. Left unresisted, hyper-engagement ultimately defeats more grounded, authentic, and valid aspirations.[2] Moreover, new technology is constantly expanding the potential reach of hyper-engagement. For example, as Niti Chatterjee and Gianclaudio Malgieri argue, the type of wearables marketed for metaverse engagement could easily "exacerbate existing areas of concern, transforming minor vulnerabilities into major threats." Along with Shabahang Arian in this volume, they presciently advance the digital vulnerability field into virtual reality.

Mateusz Grochowski's chapter also skillfully extends the scope of aspiration in the field of digital vulnerability. He convincingly argues that consumer protection laws must move beyond a purely economic focus, to address non-economic experience (including emotional and social well-be-

1 Jordan Alexander Stein, *Fantasies of Nina Simone* (Duke University Press, 2024), 11.

2 David Golumbia and Frank Pasquale, "From Public Sphere to Personalized Feed: Corporate Constitutional Rights and the Challenge to Popular Sovereignty," in *Human Rights after Corporate Personhood*, edited by Jody Greene & Sharif Youssef (Toronto: Univ. of Toronto Press, 2020).

ing). Grochowski observes that "EU consumer law has never developed a systematic framework for including non-economic interests and non-economic harm," despite an "expansion of the digital economy" that has "made this deficit particularly vivid and troublesome." This insight should be taken seriously by EU policymakers, particularly as the field of affective computing advances to develop more sophisticated methods of simulating and stimulating emotions.[3] But these same policymakers deserve credit for advancing regulation in a way that opened up space for legal academic consideration of the proper scope and force of consumer protection law.

This volume demonstrates a remarkable symbiosis between policy-oriented legal academic work, and more theoretical and philosophical scholarship. Because Europe has taken on the challenge of digital vulnerability in its privacy and consumer protection laws, it has sparked a number of fascinating inquiries into the nature of manipulation, fair trade, and commercial ethics. Meanwhile, because of the existence of this substantial body of literature, those developing new regulations and applying them are privy to deeply considered analyses of the strength and limits of the vulnerability concept. This is a virtuous cycle to which the present volume makes a sterling contribution. I congratulate the editors and authors on their remarkable capacity to refine our normative understanding of asymmetries of power and harm in online contexts, while proposing concrete advances in the legal regime meant to address these asymmetries.

3 Frank Pasquale, "Affective Computing at Work: Rationales for Regulating Emotion Attribution and Manipulation," in *Artificial Intelligence, Labour and Society*, edited by Aida Ponce del Castillo (Brussels: ETUI Press, 2024).

Vulnerability in the Digital Age

Oreste Pollicino

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PART I
Digital Vulnerability as a Paradigm for Consumer Law

Consumer Protection and Digital Vulnerability: Common and Diverging Paths

Catalina Goanta, Giovanni de Gregorio, Jerry Spanakis

A. Introduction

The past years have seen a steep increase in scholarship, public policy and civil society in the concept of vulnerability, and particularly consumer vulnerabilities on digital markets. With targeted advertising relying on mass consumer surveillance and subsequently harmful profiling, 'digital vulnerability'[1] has been presented as a concept that challenges existing understandings of European consumer protection, such as the idealised and stereotyped consumer personas introduced by the Unfair Commercial Practices Directive.[2] At the core of the argument is the consideration that the "reasonably well-informed, reasonably observant and circumspect" average consumer benchmark,[3] as well as its 'vulnerable consumer' variant focusing on personal attributes and cognitive capacities,[4] are no longer a fit for the realities of digital markets, where structural asymmetries warrant an even higher level of protection. This is due to the increasingly important assumption that "(i)n digital marketplaces, most if not all consumers are potentially vulnerable".[5] In such digital environments, it no longer

1 Natali Helberger and others, 'Structural asymmetries in digital consumer markets' (*BEUC*, March 2021) < https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf> accessed 1 March 2024.

2 Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L-149/22 (UCPD).

3 Case C-210/96 *Gut Springenheide GmbH, Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt- Amt für Lebensmittelüberwachung and Another* [1998] ECR I-4657, para. 31. See also Rossella Incardona and Cristina Poncibò, 'The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) 30 Journal of Consumer Policy 21; Hanna Schebesta and Kai Purnhagen, 'Island or Ocean: Empirical Evidence on the Average Consumer Concept in the UCPD' (2020) 28 European Review of Private Law 293.

4 Christine Riefa, 'Protecting Vulnerable Consumers in the Digital Single Market' (2022) 33 European Business Law Review 607, 611.

5 Helberger and others (fn 1) at 5.

makes sense to single out very specific groups of consumers, and use more traditional means of typification that have been crystallised in European consumer law and policy during its life-span of around 50 years. This is because everyone participating in these environments as an individual is prone to be defenceless against manipulation and exploitation.

In many ways, digital vulnerability is an accurate depiction of the risks consumers face when transacting online. One of the most debated such risks, which has already led to a wave of policy and regulatory attention around the world, is that of dark patterns. Defined as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make",[6] dark patterns are currently seen as one the biggest dangers consumers are faced with when interacting with online marketplaces. So much so, that the European Commission even ran a sweep on such practices.[7] In a study of 399 online retail shops ranging from textiles to electronic goods, it was shown that 148 websites contained at least one of three dark patterns: fake countdown timers; online interfaces "designed to lead consumers to purchases, subscriptions or other choices"; and hidden information.[8] More specifically, 42 websites were found to include fake countdown timers, 54 websites either directed consumers towards more expensive goods or options for delivery, and 70 websites were found to hide relevant information from consumers either entirely or by making it less visible.[9] The sweep builds on an earlier study launched by the European Commission showing the interest of European lawmakers in

6 Arunesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1.

7 In the policy field of consumer protection in the European Union, sweeps are wide-ranging investigations taking place at the same time in a broad number of Member States, and coordinated by the European Commission through the Consumer Protection Cooperation Network. See for instance 'Consumer Protection Cooperation Network (CPC) | Single Market Scoreboard' <https://single-market-scoreboard.ec.europa.eu/governance-tools/consumer-protection-cooperation-network-cpc_en> accessed 1 March 2024.

8 'Manipulative Online Practices' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418> accessed 4 March 2024.

9 ibid.

taming the wild west of contemporary e-commerce.[10] This interest is shared by other regulators, such as the United States Federal Trade Commission (FTC), who published a report in 2022 showcasing how "companies are increasingly using sophisticated design practices known as "dark patterns" that can trick or manipulate consumers into buying products or services or giving up their privacy",[11] by "disguising ads to look like independent content, making it difficult for consumers to cancel subscriptions or charges, burying key terms or junk fees, and tricking consumers into sharing their data".[12]

In theory, a new conception of digital vulnerability makes sense. Yet for legal reform, as we go on to argue in this chapter, it still requires a lot of theoretical and practical unpacking, as proposed regulatory solutions building on new standards of consumer vulnerability currently do not account for the broad range of infrastructural problems that can give rise to new vulnerabilities in different online consumer environments. Our contribution focuses on contextualising and critically reflecting upon digital vulnerability in two ways. First, in a concrete and very practical technology case study drawing from computational social media research, and second, through a doctrinal exploration of the potential interpretation of digital vulnerability by courts. In doing so, we put forth the view that current iterations of digital vulnerability in legal doctrine do not fully address the complexity and diversity of problems connected to platform infrastructures, and that a system-level technological rethinking of European consumer protection is necessary.

This chapter is structured as follows. The first part offers a short description of digital vulnerability,[13] as well as some popular solutions currently proposed as policy recommendations for the implementation of the concept in European consumer law and practice. The second part presents our two-pronged critique. First, we explore a computational case study

10 European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F. et al., Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report, Publications Office of the European Union, 2022 <https://data.europa.eu/doi/10.2838/859030> accessed 1 March 2024.

11 'FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers' (*Federal Trade Commission*, 15 September 2022) <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers> accessed 4 March 2024.

12 ibid.

13 Helberger and others (fn 1).

relating to vulnerability on social media, and discuss the ways in which digital vulnerability could be identified online to maximise consumer protection, albeit at the expense of other consumer rights. Second, we address the doctrinal implications of digital vulnerability vis-à-vis legal certainty by discussing the reliance of European consumer protection on judicial interpretation. The third part of the chapter synthesises the arguments under the umbrella of the critique that while conceptually fascinating, the proposed digital vulnerability notion is unsuitable to solve the problems of our current digital markets as it lacks system-level applicability, and should instead be further reframed in the light of this major limitation.

B. Digital vulnerability and structural asymmetry affecting European consumers

As briefly indicated in the introduction, the concept of digital vulnerability in consumer markets reflects a daring proposal for a paradigm shift in European consumer protection law and policy. This concept was most comprehensively articulated in a 2021 report of the European Consumer Organisation (BEUC).[14] With consumer harms arising at unprecedented pace and scale from business practices such as targeted advertising based on consumer profiles, price discrimination and dark patterns,[15] digital vulnerability is presented as a necessary answer to the growing concern that existing levels of consumer protection are insufficient in addressing these harms.

Consumer vulnerability has long been a topic of consumer research. A literature review looking at 25 years of post-modern practices in marketing across 859 published articles, revealed four major research themes on this topic: "marketing, fraud and consumers; consumer vulnerability and well-being; ethics and vulnerable consumers; and consumption, disability and gender".[16] The first theme was associated mostly with research on financial services, persuasion and low-income consumers. The second theme addressed children, poverty, subsistence marketplaces and effects on well-

14 ibid.

15 ibid at 6.

16 Rituparna Basu, Anil Kumar and Satish Kumar, 'Twenty-five Years of Consumer Vulnerability Research: Critical Insights and Future Directions' (2023) 57 Journal of Consumer Affairs 673.

being. The third cluster of publications generally dealt with corporate social responsibility, elderly consumers, sustainability and consumer behaviour. Lastly, the fourth research theme tackled consumer issues focused on disability, gender, identity and motherhood.[17] These thematic research clusters mirror the more traditional understanding of vulnerability as crystalised in existing legislation. For instance, as the BEUC report also highlights, according to the UCPD, consumers "can be considered vulnerable because of their personal characteristics, namely mental or physical infirmity, age or credulity",[18] leading to a "vantage point from which commercial practices can be assessed",[19] by identifying consumers or groups of consumers who may be more prone to manipulation and harm. The report discusses arguments from multidisciplinary vulnerability scholarship that distinguishes vulnerability from victimization and victimhood,[20] seen as "unnecessarily stigmatising, patronising and disconnected from social reality",[21] as consumer vulnerability "is a sometimes misunderstood or misused concept that is equated erroneously with demographic characteristics, stigmatization, consumer protection, unmet needs, discrimination, or disadvantage".[22] At the same time, the report also points to other opinions aiming to limit a more universal understanding of consumer vulnerability as being too all-encompassing, given the vast implications of diverse vulnerabilities at individual level.[23]

The report shapes the concept of digital vulnerability around a series of proposed characteristics. First, digital vulnerability must take into account the conceptual refinement of the notion of vulnerability itself, as we ought to differentiate between sources and states of vulnerability, where the former can be inherent (intrinsic to the human condition) and situational (arising in a particular context or situation), while the latter can be dispositional (potential) and occurrent (dispositional vulnerabilities that

17 ibid; See also Ronald Paul Hill and Eesha Sharma, 'Consumer Vulnerability' (2020) 30 Journal of Consumer Psychology 551.

18 Helberger and others (fn 1) at 9.

19 ibid.

20 Alyson Cole, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique' (2016) 17 Critical Horizons 260.

21 Helberger and others (fn 1) at 10.

22 Stacey Menzel Baker, James W Gentry and Terri L Rittenburg, 'Building Understanding of the Domain of Consumer Vulnerability' (2005) 25 Journal of Macromarketing 128.

23 ibid at 11.

manifest themselves).[24] Second, seeing the data-driven nature of online markets, digital vulnerability is architectural and it reflects the properties of digital architectures.[25] Third, digital vulnerability is relational because of the way in which consumers interact with one another and with the influences of commercial parties.[26] Fourth, lack of privacy can be seen as a potential source of vulnerability, given the nature of "data-driven practices that promote exploitation of vulnerabilities".[27]

Some of the concrete recommendations made in the BEUC report reflect concrete proposals for regulatory reform, as "the law on unfair commercial practices has to be rethought in order to remain a useful tool in the fight against digital asymmetry".[28] Reform proposals include the anchoring of digital vulnerability and digital asymmetry in the UCPD (e.g. Articles 5, 8 and 9), the reversal of the burden of proof "as a necessary consequence of the way in which new technology is used to manipulate the consumer through all sorts of marketing strategies",[29] or the blacklisting of additional commercial practices as a self-standing category of digital practices.[30] Other recommendations propose regulatory co-design, such as concretising legal benchmarks in guidelines co-created by businesses, consumers and enforcement authorities.[31]

This brief overview of how digital vulnerability is proposed in the BEUC report aims to bring into discussion the very valuable and innovative conceptual framing presented in the study, with which the authors undoubtedly make significant contributions to existing scholarship. The characteristics of digital vulnerability presented therein reflect very persuasive arguments that warrant the reconsideration of whether the current legal understanding of vulnerability is socially, economically and also technologically decrepit. This reconfiguration, focused on the particular context of consumers who may be vulnerable in different ways at different moments throughout their lives, is reminiscent of theories of personalised law, which equally hold that the law should apply in a bespoke manner to individuals, as opposed to the standardisation and typification that legal systems around the world gener-

24 ibid at 16-17.
25 ibid at 18.
26 ibid at 20.
27 ibid at 23.
28 ibid at 76.
29 ibid.
30 ibid at 79.
31 ibid.

ally work with.[32] Yet just like personalised law, in spite of its conceptual attractivity, digital vulnerability does not come across as very practical, particularly when linked to policy recommendations that do not really rethink the nature of consumer protection, but merely continue the established tradition of troubleshooting and patchworking the European consumer *acquis*. In the next section, we explore to what extent the articulation of a new concept of consumer digital vulnerability in the real-world might deliver on its promised value.

C. The ever-expanding complexity of digital vulnerability

As the European Union explores regulatory reforms to develop strengthened protections for individuals on digital markets, the digital vulnerability framework has gained a lot of traction in both (legal) scholarship and policy-making circles. Whether such a framework will be embedded in, for instance, the expected reform of the UCPD following the Commission's Fairness Fitness Check, remains to be seen.[33] Between contracted studies,[34] public consultations[35] and the rising volume of consumer research on vulnerability, the Commission could make very sensible proposals as to why there should be additional changes to the UCPD even as early as five years after the upgrades introduced by the Modernisation Directive.[36] The public consultation on the Fitness Check, comprising 350 online responses to a questionnaire and 71 position papers, revealed some wide-spread consumer

32 Omri Ben-Shahar and Ariel Porat, 'Personalizing Mandatory Rules in Contract Law Symposium: Personalized Law' (2019) University of Chicago Law Review 255; Christoph Busch, 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law Symposium: Personalized Law' (2019) University of Chicago Law Review 309.

33 'European Commission - Have Your Say' (*European Commission - Have your say*, 14 June 2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 5 March 2024.

34 Lupiáñez-Villanueva and others (fn 10).

35 'European Commission - Have Your Say' (n 33).

36 Directive (EU) 2019/2161 of the European Parliament and of the Council 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 L 328 (Modernisation Directive).

issues around dark patterns in general, as well as subscription cancellation difficulties and a lack of disclosures of paid promotions in particular.[37]

It is noteworthy that the Fitness Check has a broader scope of reflection than most of the literature available on (digital) consumer vulnerability. Consumer protection is traditionally discussed in the context of marketplaces and e-commerce.[38] Yet other digital industries are equally embracing e-commerce in even more complex and opaque online architectures than the checkout interfaces of websites like Amazon or Shein. One of the core industries where this trend has been visible in the past years already is social media. Social commerce reflects the integration of e-commerce on social media.[39] This trend has been shaping social media in at least two ways.

On the one hand, new content monetisation products launched by social media platforms are proliferating contractual interactions between traders and consumers. An example in this respect is the TikTok Shop, launched in September 2023, offering users the opportunity to sell goods through designated e-commerce interfaces pertaining to TikTok, which are often linked to content production on LIVE shopping.[40] Put differently, platforms like TikTok are starting to offer new iterations of teleshopping services, where instead of calling a number to buy a pan seen on television, a consumer has to navigate a complex ecosystem of social media affordances (e.g. the Shop Tab, Product Showcase, In-Feed Video and Live Shopping, Shop Ads) and indirect interactions with other data brokers in the e-commerce supply chain (e.g. affiliate networks, commerce platform partners, multi-channel partners, dropshipping intermediaries) to buy a product.

On the other hand, products promoted on social media are not just merely listed on product pages, but also featured in commercial content that is generally underdisclosed as such.[41] The drivers of this new form

37 'European Commission - Have Your Say' (n 33).

38 Mathur and others (n 6).

39 Christine Riefa, 'Consumer Protection on Social Media Platforms: Tackling the Challenges of Social Commerce' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law in the Digital Era* (Springer International Publishing 2020) <https://link.springer.com/10.1007/978-3-030-25579-4_15> accessed 8 February 2023.

40 'Introducing TikTok Shop' (*Newsroom | TikTok*, 12 September 2023) <https://newsroom.tiktok.com/en-us/introducing-tiktok-shop> accessed 5 March 2024.

41 'Results of a Screening ("Sweep") of Social Media Posts' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_708> accessed 5 March 2024.

of native advertising are influencers and content creators, an emerging stakeholder group attracting and keeping audiences on social media. The connection developed between creators and their audiences, referred to as parasocial relationships,[42] are rooted in the familiarity, authenticity and relatability that content creators can offer to their online followers. Parasocial relationships are also full of emotions, leading followers to admire and defend the choices of their favourite Internet celebrities. These features nurture consumers' trust in the recommendation and review of products and services.[43] The content creation global market is expected to reach half a trillion dollars by 2027.[44] Given that it brings together the three most popular activities Internet users currently enjoy online, namely social networking, content streaming and shopping,[45] the content creation economy warrants much more attention in terms of consumer protection pitfalls. This should not be limited to questions of digital addiction,[46] but also include clarifying how consumer law applies to digital content and services shaped by the content monetisation strategies of social media platforms.[47]

The Fairness Check addresses some of the risks of undisclosed advertising by social media influencers, but does not fully acknowledge the

42 See for instance Amanda N Tolbert and Kristin L Drogos, 'Tweens' Wishful Identification and Parasocial Relationships With YouTubers' (2019) 10 Frontiers in Psychology 2781.

43 For a comprehensive overview on the influence of influencers see Frithjof Michaelsen et al, 'The impact of influencers on advertising and consumer protection in the Single Market' (Study requested by the IMCO committee, European Parliament, February 2022) <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703350/IPOL_STU(2022)703350_EN.pdf>. See also Marijke De Veirman, Liselot Hudders and Michelle R Nelson, 'What Is Influencer Marketing and How Does It Target Children? A Review and Direction for Future Research' (2019) 10 Frontiers in Psychology 2685.

44 'The Creator Economy Could Approach Half-a-Trillion Dollars by 2027' (*Goldman Sachs*, 29 February 2024) <https://www.goldmansachs.com/intelligence/pages/the-creator-economy-could-approach-half-a-trillion-dollars-by-2027.html> accessed 5 March 2024.

45 Vibhor Agarwal and Nishanth Sastry, '"Way Back Then": A Data-Driven View of 25+ Years of Web Evolution', *Proceedings of the ACM Web Conference 2022* (ACM 2022) <https://dl.acm.org/doi/10.1145/3485447.3512283> accessed 9 July 2022.

46 'New EU Rules Needed to Address Digital Addiction | News | European Parliament' (12 December 2023) <https://www.europarl.europa.eu/news/en/press-room/20231208IPR15767/new-eu-rules-needed-to-address-digital-addiction> accessed 5 March 2024.

47 Taylor Annabell, Catalina Goanta and Sophie Bishop, '"You and TikTok are, and will remain at all times, independent contractors": Classification of influencers and monetisation practices in TikTok documentation', forthcoming 2024.

fundamental business model shifts social media platforms are undergoing through the further development of monetisation.

These emerging ecosystems raise their own challenges for digital vulnerability, with far stretching implications that lead to further interpretation issues. How will the dark patterns discussion be extended to social media interface features? How should we distinguish between the impact of interface architectures and other manipulative influences such as parasocial relationships which rely on emotional manipulation? Should we distinguish between individual instances of vulnerability and clusters of practices that may enhance the severity of vulnerability? These are only a handful of questions unveiling the complexity of the topic.

So far, consumer literature on vulnerability has focused on making theoretical contributions to the understanding of this problem, aiming to conceptualise some of the notable shifts in what our legal understanding of consumer harms ought to be. In what follows, this chapter will complement existing analyses with two more applied perspectives: one focused on specific industry practices in the social media sector, and another focused on judicial practices around the interpretation of consumer protection in Europe.

I. Case study: monetising conspiracy theories on YouTube

To exemplify the complexities of digital markets, this subsection describes and discusses concrete instances and dimensions of vulnerability in relation to social media monetisation, by unpacking a 2022 study on the monetisation of YouTube conspiracy theories.[48]

1. A brief introduction to monetisation

Before delving into the study itself, it is important to first revisit the monetisation discussion and briefly set the scene around social media monetisation. Consumer markets where more traditional transactions have been moved to the online world (e.g. selling and buying consumer goods)

48 Cameron Ballard and others, 'Conspiracy Brokers: Understanding the Monetization of YouTube Conspiracy Theories', *Proceedings of the ACM Web Conference 2022* (ACM 2022) <https://dl.acm.org/doi/10.1145/3485447.3512142> accessed 4 March 2024.

have their own challenges and transformations, such as the rise of intermediation, opaque targeting, etc. However, as emerging transactional environments, social media platforms bring with them even more complexity. In this context, monetisation can be interpreted to refer to two types of economic practices. On the one hand, monetisation drives the development of new business models by social media platforms. For instance, the displaying of ads on YouTube channels – known as YouTube AdSense[49] - has been one of YouTube's most famous business model around user-generated content. In more recent years, YouTube has been diversifying its monetisation approaches by for instance partnering up with Shopify and enabling users to purchase goods and services while they are featured in videos.[50] Additional developments include for instance BrandConnect, the platform solution for the intermediation of influencer marketing.[51] These are examples of monetisation products developed by YouTube to diversify its revenue streams by tapping into and shaping new socio-cultural phenomena and consumer needs. On the other hand, monetisation also reveals the economic incentives of other stakeholders in digital supply chains. This includes legitimate economic actors such as creators, brands, advertising agencies, etc., but also illegitimate actors such as scammers and criminal organisations. Monetisation products made available by platforms can be bundled into what we can call as 'monetisation portfolios', namely a variety of business practices enabling these economic actors to produce revenue across a wide range of platforms and monetisation opportunities, making them more resilient to losing any one particular revenue stream.

2. Monetising conspiracy channels

Ballard et al. investigated the monetisation 'methods' of a specific category of YouTube channels, focused on conspiracy theories. In doing so, researchers collected information about the ads delivered on these channels, as well as any other information they could gather from the description of the videos. Starting with advertising, they identified three types of advertising

49 See Google FAQs <https://support.google.com/youtube/answer/11602441?hl=nl> accessed 4 March 2024.

50 'Sell to Customers on Google and YouTube' (*Shopify*) <https://www.shopify.com/google> accessed 1 April 2024.

51 'BrandConnect for Influencer Advertising - YouTube Advertising - YouTube Advertising' <https://www.youtube.com/ads/brandconnect/> accessed 1 April 2024.

on YouTube: video ads "served before or during a video"; "advertisements on the video sidebar"; and "banner ads in the middle of videos that do not interrupt viewing".[52] Researchers emphasise that these ads are part of YouTube's ad delivery system, which allows advertisers to "upload a combination of text, images and video" and "specify on which sites or apps the advertisement can be seen and how the ad should be targeted", in exchange for specifying "the amount of money they are willing to spend per interaction with an ad, referred to as a bid".[53] The research team also specifies that Google controls the process determining when and where the ads will be served, "through a combination of content restriction, bidding and personalisation", and that ad personalisation entails the targeting of audiences on the basis of "personal demographics or interests of the viewer", as well as "ad context, i.e. where the ad is shown".[54]

To investigate the advertising monetisation models, the study set up two different datasets: a conspiracy dataset focused on 818 YouTube channels, where 43,379 ad impressions were extracted from 93,443 videos; and a control dataset amassing 11,912 channels, 140,839 ad impressions and 47,847 videos. The conspiracy channel list was sourced in two ways. First, by relying on a labelled YouTube channel dataset from an earlier political study,[55] and second, by identifying further conspiracy channels based on shared subscribers.[56] The findings showed that certain types of ads are more common in the conspiracy dataset, such as self-improvement ads (e.g. advertising 'webinars, books or courses promising an easy route to financial independence'[57]), lifestyle and alternative health ads, as well as low-quality gadgets and beauty products. With an additional check of the domain names (URLs) associated with predatory ads, the research team found that "ads [...] identified as deceptive or predatory accounted for 15% of all impressions in the conspiracy set, but only 1.4% of control impressions. Ad content ranged from get-rich-quick schemes, to promises of immortality through essential oils, to 5G-proof un- derwear".[58]

52 Ballard and others (n 48).
53 ibid.
54 ibid.
55 Mark Ledwich and Anna Zaitsev, 'Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization' [2020] First Monday <https://journals.uic.edu/ojs/index.php/fm/article/view/10419> accessed 1 April 2024.
56 Ballard and others (n 48).
57 ibid.
58 ibid.

The study also revealed other business models used by the owners of conspiracy channels on YouTube. Based on an analysis of the video descriptions of the collected videos, researchers were able to identify that monetisation models focused on requesting donations (e.g. Patreon, GoFundMe), selling merchandise directly to consumers, or directing consumers to additional websites with alternative monetised content (e.g. 'free speech' platforms such as Rumble) were also prevalent in the conspiracy dataset. This is evidence of the complexity of the 'monetisation portfolio' mentioned above, where economic operators (whether in good or bad faith) cluster a wide array of practices meant to bring them revenue.

3. Relevance for the digital vulnerability debate

The study referred to in this section is an important example of how consumer vulnerability is exploited in the practice of social media content monetisation, not only by bad faith actors, but also by platforms themselves. This happens in at least three layers of commercial activity. First, YouTube channels with specific content are set up – in this case conspiracy theories. Such theories can range across a wide amount of topics and may be more or less grounded in science, but what is most important is that they bring together a homogenous audience based on the interest of viewers in that specific content. Here, consumers are viewers. Second, YouTube channels are primarily monetised through advertising, and the ads shown on conspiracy channels target users based on demographic data and content interest. The channels displaying such ads earn advertising revenue through YouTube, and the companies buying targeted advertising are able to deliver fraudulent goods and services to audiences, as consumers become potential purchasers of these goods and services. Third, conspiracy channels themselves may re-direct viewers to additional websites promoting fraudulent product or service offers, turning viewers once more, into potential buyers or donors for specific causes. The second and third layers of commercial activity (monetisation through advertising; and monetisation through selling/donations) link the content of YouTube channels, which may be persuasive and very much based on extracting emotional reactions from audiences, to transactions that consumers may immediately engage in. For the sake of visualising how this works, imagine watching a conspiratorial video about vaccinations, aimed to instil fear and rally support against public policies related to vaccination, only for the video description to contain specific products recommended to replace vaccination, and which are

directly ready to purchase at the click of a few buttons. This transactional simplification showcases a dual vulnerability for consumers: noy only is the specific group of conspiracy-loving consumers easily identifiable as the audience of specific YouTube content, but it also becomes subsequently targeted (whether via YouTube's personalisation or the channel's monetisation itself) with additional harmful commercial practices.

4. Contextual vulnerability: technical solutions for complex social media consumer harms?

It is not the purpose of this section to delve into a comprehensive application of European consumer protection to the consumer harms scenarios arising out of the conspiracy study described and analysed above. Still, it can be reasonably argued that to the extent European consumers viewing conspiracy videos on YouTube channels would also be exposed to goods and products advertised using incorrect scientific and factual claims, they may generally be considered unfair under the UCPD. In principle, and depending on the procedural implementation of the UCPD in different Member States, consumers may have – among others – tort-based remedies to alleviate the damages suffered by engaging in snake oil transactions (e.g. fake medicinal products). Moreover, national authorities tasked with the enforcement of consumer protection may dispose administrative sanctions such as fines and injunctions to stop the proliferation of harmful practices. Yet in this case, the UCPD would very likely lead to the limitation that sanctions and remedies have not traditionally been targeted at platforms, but instead, at advertisers and sellers themselves. In this case, it would entail that consumers and authorities would have to identify and take legal action against the owners of channels, as well as advertisers who may engage in unlawful conspiratorial advertising and selling. This is due to the fact that the UCPD was not designed as a platform instrument, but has rather focused on more direct transactional relationships between traders and buyers. And while it is true that YouTube is itself a trader vis-à-vis European consumers, applying the UCPD in its current shape to the case study described above would only – at best – attract YouTube's liability with respect to this relationship between itself and consumers as viewers/users of the platform.

So how could YouTube actually take into account contextual consumer vulnerability? As a platform collecting every click and action taken by

users while engaging with its products, YouTube has the necessary data points to identify for instance when a specific user goes on a conspiracy binge, and when such a binge would be followed by engagement with third party websites. Particularly if consumers use in-app browsers (e.g. using YouTube on a mobile phone and clicking on external websites from there), YouTube would in principle also be able to collect shopping data about the consumer.[59] Assuming YouTube could detect and determine links between the consumption of emotional content and the purchasing of problematic goods or services, it could impose for instance limitations on monetisation by the channel owners or advertisers. Demonetisation, seen as removing the possibility of making revenue by YouTube channels, is an approach that YouTube is already using to limit problematic content. However, what exactly is problematic content? Even for authorities and courts, drawing the line between safe and unsafe products, or holistic medicine and snake oil is no easy task – and neither is determining when a consumer may be contextually vulnerable. As a result, while YouTube may have a lot of power and information about its users, identifying and proactively protecting vulnerable consumers entails setting private governance standards that may not always perfectly align with the law. Is placing the burden on YouTube to replace our judiciaries and public administration institutions on determining, on a case by case basis, what is a good product and what is a bad product, the way ahead? Or do we need to bring the focus back from the private governance by platforms to public governance through European harmonisation and judicial interpretation? The next section segues into this latter point.

II. Revisiting the harmonisation debate through judicial interpretations of European consumer protection

Traditionally, European consumer protection has heavily relied on judicial interpretation for the development of its core concepts. This is due to the fact that while it has a long standing history in European law and policy, consumer protection legislation has fuelled a lot of political and doctrinal

59 'iOS Privacy: Instagram and Facebook Can Track Anything You Do on Any Website in Their in-App Browser' (*Felix Krause*, 10 August 2022) <https://krausefx.com//blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser> accessed 1 April 2024.

disagreement in relation to its goals and practical implications. An example in this respect is the Unfair Contract Terms Directive and its 'irritating' effect on UK law, beautifully captured in Teubner's analysis from a few decades ago,[60] as one of the many discussions relating to how consumer harmonisation has not been without its own discontents at national and supranational level, in policy as well as in academia.[61]

The harmonising impact of consumer protection legislation must be once more revisited in the context of digital vulnerability: as the complexity of market practices and architectures grows exponentially, is it reasonable to rely on patchwork regulation to address transnational, complex platform systems with the goal of protecting against legally uncertain, contextual vulnerabilities? European consumer protection law remains inherently dependent on judicial interpretation for its effectiveness – a feature that not even the UCPD managed to change, in spite of its annex of prohibited commercial activities. This interpretation, in turn, remains bound by national preferences and practices, but most importantly – remains also case-specific. In other words, the scalability of judicial interpretation is modest at best, even when flowing from the European Union's highest court.

To shed some further light on interpretational issues, we draw on the empirical study conducted by Schebesta and Purnhagen on the concept of the average consumer.[62] This 2020 study, combining doctrinal and empirical methods, aimed to understand how the UCPD average consumer test is applied by the CJEU, by systematically analysing 12 relevant cases with a clear application of the average consumer concept, and finding that the "empirical analysis revealed the muddy nature of the Court's legal

60 Gunther Teubner, 'Legal Irritants: Good Faith in British Law or How Unifying Law Ends up in New Divergences' (1998) 61 The Modern Law Review 11.

61 Roger Van Den Bergh, 'The Uneasy Case for Harmonising Consumer Law' in Klaus Heine and Wolfgang Kerber, *Zentralität und Dezentralität von Regulierung in Europa* (De Gruyter 2007) <https://www.degruyter.com/document/doi/10.1515/9783110511260-009/html> accessed 1 April 2024; Marcus Klamert, 'What We Talk About When We Talk About Harmonisation' (2015) 17 Cambridge Yearbook of European Legal Studies 360; Onyeka K Osuji, 'Business-to-Consumer Harassment, Unfair Commercial Practices Directive and the UK—A Distorted Picture of Uniform Harmonization?' (2011) 34 Journal of Consumer Policy 437; Simon Whittaker, 'Unfair Contract Terms and Consumer Guarantees: The Proposal for a Directive on Consumer Rights and the Significance of "Full Harmonisation"' (2009) 5 European Review of Contract Law 223; Hans-W Micklitz, 'Minimum/Maximum Harmonisation and the Internal Market Clause', *European Fair Trading Law* (Routledge 2006).

62 Schebesta and Purnhagen (n 3).

reasoning about the average consumer benchmark".[63] What is more, the authors also posited that the average consumer test of the UCPD had led to an isolated interpretation when considering other areas of European law, and that it ultimately relies on the further interpretation of national courts.

This study is essential in understanding the slow and convoluted process of judicial interpretation in the context of supranational governance and harmonisation policies, even when addressing a rather popular instrument that has led to a lot of case law both at European and national level. Moreover, attention should also be paid to the fact that the judicial interpretation by the CJEU is deemed to be 'muddy' even in the context where one Court has had a little under 20 years to build on its understanding of a fundamental concept for the operation of the UCPD.

So what does this mean for new concepts of consumer vulnerability? In short, new substantive formulations of consumer vulnerability, such as contextual vulnerability, will not solve digital asymmetries – or at a minimum will not solve them fast enough – because of the shortcomings of judicial interpretation. This argument can be unpacked along two such limitations. First of all, contextualising vulnerability in the meaning that anyone can be vulnerable on the Internet[64] entails understanding the specific situations in which a consumer may find themselves vulnerable. The idea of breaking the boundaries of legal stereotypification (e.g. based on age or credulity as insufficient determinants of vulnerability) may have great theoretical value, but at the same time it may open the door to an overwhelming amount of individually personalised parameters and combinations of parameters which may be very specific to the circumstances of individual consumers. In this case, even with the CJEU guiding the abstract interpretation of novel concepts, the filling of these concepts by national courts could very well lead to a complete collapse of harmonisation as we know it. Second of all, even if more systematic approaches can be found to avoid the over-personalisation of vulnerability (e.g. by adding new, specific vulnerability determinants), judicial interpretation clarity only comes with high volumes of case law which would take a very long time to develop in legal practice. As a result, it is unclear to what extent such a solution would address the problems of legal uncertainty embedded in the application of a legislative instrument whose innate flexibility has already led to 'muddy' interpretations.

63 ibid at 308.

64 Helberger and others (fn 1) at 25.

Overall, given the reliance of European consumer protection on judicial interpretation, current legislation such as the UCPD simply does not lend itself to the scalability that is required when aiming to effectively solve consumer harms on a broad range of digital markets, even though the need for this scalability is arguably a part of the structural asymmetry discussion. Perhaps most importantly, to the extent that they are divorced from market knowledge about commercial practices across all relevant sectors, as exemplified in Section 3.1, novel frameworks of consumer vulnerability will not be sufficient to further patchwork European consumer protection legislation into more effective application.

Instead, a complete overhaul of the goals of European consumer protection legislation such as the UCPD might be necessary. Literature on platform governance – and particularly on content moderation – has been advancing the argument that the focus on individual cases and interpretations characterising today's jurisdictions in relation to unlawfulness in digital environments such as social media platforms is a 'mistake'.[65] The next and last section elaborates on this argument and applies it to digital vulnerability framework.

D. Synthesis and conclusion: digital vulnerability and the need for systems-thinking

In a recent paper on content moderation and US constitutional law, Douek forwards the argument that legal decision-making in the context of scaled, complex systems such as social media platforms ought to fundamentally shift from an individual case basis to 'mass speech administration'. This is due to the fact that "the vehicle of individual error correction" allowed for by judicial and doctrinal interpretations of constitutional legal standards in the US is no longer fit to deal with the "complex and dynamic system" of platform governance, and it should be replaced with what the paper calls "a second wave of regulatory thinking about content moderation institutional design that eschews comforting but illusory First Amendment–style analogies and instead adopts a systems thinking approach".[66] This argument builds on earlier iterations of critiques around the fitness of traditional legal

65 Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) 136 Harvard Law Review 526, 532.

66 ibid.

systems in governing speech online, such as those proposed by Balkin and Langvardt, who drew attention to the process of administratively managing content moderation at unprecedented scale.[67]

This argument neatly applies to any interaction between traditional legal thinking and complex digital commercial ecosystems. So what would systems-thinking look like in the context of applying European consumer protection at scale? This chapter does not aim to provide a comprehensive analysis of this question, but rather exemplify a few directions this discussion could further take, particularly at the intersection of literature on platform governance and consumer protection. To open the appetite for such theoretical incursions, two points are briefly addressed: the need to develop cohesive platforms-as-systems obligations under the European consumer *acquis*; and the classification of consumer protections based on their potential technological operationalisation at scale.

In terms of the first point, even after the Modernisation Directive, the UCPD and its tests – including the existing conception of consumer vulnerability – have generally not focused on platforms as intermediaries. The few exceptions which can be observed in the updated Annex include obligations for search engines (point 11a),[68] as well as obligations for platforms displaying consumer reviews (points 23 b and c).[69] Although as such, platforms themselves may be traders, the UCPD does not explicitly acknowledge the role of platforms in collecting and intermediating information. For instance, while the application of the UCPD to influencer marketing practices around advertising disclosures has been unquestionably established, the discussion has generally focused on the obligation of influencers as traders in making such disclosures. However, it can be argued that platforms themselves, through interface design and architectures, make it difficult for disclosures to be properly made or displayed. Still, to date, the role of platforms in the policy process around the regulation of influencer marketing from a consumer perspective remains minimal. Particularly in

67 ibid.

68 Point 11a, UCPD Annex: "Providing search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results."

69 Point 23b, UCPD Annex: "Stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers"; Point 23c, UCPD Annex: "Submitting or commissioning another legal or natural person to submit false consumer reviews or endorsements, or misrepresenting consumer reviews or social endorsements, in order to promote products."

the case of new frameworks around digital vulnerability, platforms should have a central role not only in reshaping the substance of legal standards, but also in terms of their procedural application. This discussion will have to also involve growing concerns relating to the cohesion of the European consumer *acquis*.

With the adoption of the Digital Services Act, which includes a lot of relevant provisions for consumers, and which is deemed a systems regulation, European law now faces the difficult task of aligning existing sectoral rules with the newly emerged digital *acquis*.[70] This does not only entail aligning interpretations across instruments, but also making sure that legal obligations do not conflict. Would imposing more consumer obligations on platforms be a permitted deviation from the liability exemptions platforms may enjoy under the DSA? If we consider consumer protection legislation as *lex specialis*, that should be indeed the case. In addition, the interpretation of 'illegal content' in the light of the consumer acquis is another aspect of this legislative interaction which ought to be clarified in the coming years.

However, while the notion of illegal content is left to the law of Member States, it is not the same for harmful content for consumers which, despite legal, are left in the decision-making process of online platforms. Proposing a certain diet or lifestyle is not illegal per se but it could lead to users' distress and addiction. Even influencing public opinion by relying on political speech to hide strategies of content monetisation does not qualify as an illegal conduct, but it can be harmful for democracy. This grey area for consumer law is left to online platforms which, in case of Very Large Online Platforms (VLOPs), can consider this issue as a system risk based on Article 34 DSA if considering that consumer protection is a fundamental right protected by the European Charter.

More broadly, the DSA can be conceived as the starting point of a regulatory 'administrativisation' of content moderation. The European reaction to platform governance has led to the introduction of procedural safeguards which aims to protect users in the process of content moderation. Nonetheless, the scale and quantity of the activity in content moderation has already underlined the potential limit of these safeguards, including transparency and disclosure for consumers, which now have access to billions of entries, just when referring to the obligation of statement of reason based on Article

70 Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) European Journal of Risk Regulation 1.

15 DSA. This framework leads to thinking more about the process of content moderation in a systematic way, and, therefore, requires enforcement authorities to think in the same direction.

This moves us to the second point regarding the operationalisation of consumer protection obligations at scale. A quick look at the DSA Transparency Database,[71] which also includes marketplaces and not only social media platforms in terms of compliance with the transparency requirements in Article 17 DSA (e.g. submitting content moderation decisions in a publicly available database), reveals that most content moderation decisions are actually made by marketplaces such as AliExpress. On marketplaces, content moderation often takes the form of policing unsafe and illicit products. While some interpretational issues may still exist around determining which products may be lawfully sold, product safety practices have led to the development of databases such as Safety Gate,[72] where national consumer authorities report unsafe products in an agile manner, which can be prone to further operationalisation by large online marketplaces, through, for instance, API implementation.[73] This is a concrete expression of the administrative dimension of systems-thinking such as that put forth by Douek. Furthering this perspective can entail classifying consumer protection obligations on the basis of whether they can be technically implemented or not. Information duties in the consumer *acquis*, trader registration are examples of obligations that can easily be implemented in the architectures of platforms, with the advantage of automating compliance checks as well. This is due to their administrative registration nature, which does not leave that much leeway for subjective interpretation. Whether consumer digital vulnerability can be automated at all, remains to be seen. Most likely, some aspects of it should be straight forward to platforms. For instance, YouTube should already restrict certain types of advertising on channels dedicated to children. A 'Safety Gate' for children advertising topics (including products), that could allow national authorities to set out constantly updating limitations would be another example of technically embedding legal standards on platforms at a systems level.

71 See <https://transparency.dsa.ec.europa.eu>.

72 See < https://ec.europa.eu/safety-gate-alerts/screen/webReport>.

73 Catalina Goanta, Thales Bertaglia and Adriana Iamnitchi, 'The Case for a Legal Compliance API for the Enforcement of the EU's Digital Services Act on Social Media Platforms', *2022 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2022) <https://dl.acm.org/doi/10.1145/3531146.3533190> accessed 1 April 2024.

Neither of the two ideas elaborated above are perfect solutions to the problem of complexity around consumer vulnerability on digital markets. However, what this chapter has aimed to achieve is a brief demonstration that without taking into account the system-level nature of transnational superplatforms, and adapting consumer protection accordingly, we are not sufficiently addressing the new world of digital markets. Although theoretically fascinating, digital asymmetries and contextual vulnerabilities will not be solved by exclusively increasing the standard of substantive consumer protection, or by adding new procedural safeguards in traditional judicial processes. Instead, focusing on the responsibility of platforms to adapt to and interact with European consumer protection standards at infrastructural level ought to be the focus of regulatory reforms that should technically rethink the role of consumer protection in the digital sphere.

Investigating Digital Vulnerability with Theories of Harms: A Methodological Proposal with Three Illustrations

Fabrizio Esposito

A. Overview

If one asks ChatGPT-3.5 to "write 300 words on the word 'vulnerability'. Discussing in particular its etymology and its relation with the word 'harm'", ChatGPT-3.5 answers as follows:

"The word 'vulnerability' is a powerful and multifaceted term that encompasses the essence of human existence. Its etymology traces back to the Latin word 'vulnerabilis', derived from 'vulnerare', meaning 'to wound' or 'to injure'. This linguistic lineage highlights the core concept behind vulnerability – a susceptibility to harm or injury. The term has evolved over centuries, but its fundamental meaning remains rooted in the idea of being exposed to potential harm.

Vulnerability is a concept deeply intertwined with the word "harm". It signifies a state of fragility or weakness that makes individuals or entities more susceptible to experiencing harm, whether physical, emotional, or psychological. The relationship between vulnerability and harm is intricate and vital for understanding human experiences and relationships.

In the realm of psychology and emotional well-being, vulnerability is often associated with opening oneself up to the possibility of emotional harm. It is the act of allowing one's true self to be seen, which can lead to profound connections with others but also exposes one to the risk of rejection or hurt. This concept is at the core of Brené Brown's work on vulnerability, where she posits that embracing vulnerability is essential for building genuine connections and resilience.

In the context of social justice and equity, recognizing and addressing vulnerability is crucial. Vulnerable populations, such as marginalized communities or individuals facing economic hardship, are more susceptible to harm in various forms, including discrimination, injustice, and unequal access to resources. Acknowledging vulnerability in these contexts is essential for advocating for fairness and equal opportunities.

In essence, vulnerability is an intrinsic aspect of the human condition, deeply intertwined with the concept of harm. It reminds us that, in our pursuit of personal growth, connection, and justice, we must acknowledge and address the vulnerabilities within ourselves and in others. By doing so, we can foster empathy, compassion, and resilience, ultimately striving for a more inclusive and understanding world".[1]

This short text is accurate. Moreover, it provides two relevant insights. The first is that the digital environment is undeniably a source of opportunity. At the same time, it is also a source of concern. The second is that the idea of vulnerability is intrinsically connected with the idea of harm. Accordingly, this chapter will provide an overview of an approach to consumer law and policy called 'theories of harm'.

More precisely, the approach will be presented in general terms. Next, the uses of this approach will be discussed and exemplified. Finally, the chapter will investigate three applications of the theory that are particularly relevant for future research concerning digital environments: hidden gems and hidden traps in digital marketing; hyper-engaging practices; personalized prices and personalized terms more generally.

B. What is a theory of harm, and why the study of vulnerability needs one

The idea of theories of harm is mainstream in the practice of competition law.[2] In the context of consumer law, instead, its relevance is becoming to be recognized.[3] Being a recent idea, it has yet to receive the attention

1 https://chat.openai.com/share/769019ff-1810-481b-9c69-9ea4c760a7b4, last access: 30 October 2023.

2 For a nuanced discussion, see Jan Broulík, 'Relevant Generality of Antitrust Economics: Competitive Effects as Adjudicative and Legislative Facts' (2023) 19 Journal of Competition Law & Economics 444. For examples of theories of harm related to digital markets, see Jan Kraemer and Daniel Schnurr, 'Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies' (2023) 18 Journal of Competition Law & Economics255; Massimo Motta, 'Self-Preferencing and Foreclosure in Digital Markets: Theories of Harm for Abuse Cases' (2023) 90 International Journal of Industrial Organization 102974; Avdasheva Svetlana and Korneeva Dina, 'Theories of Harm for Multi-Sided Platforms: Challenges for Competition Policy and BRICS Answers'; OECD 'Theories of Harm for Digital Mergers', https://www.oecd.org/competition/theories-of-harm-for-digital-mergers.htm, accessed 29 October 2023.

3 Seminal, in this regard, is the monograph by Harriet Gamper, Paolo Siciliani and Christine Riefa, *Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making* (Hart Publishing 2019).

it deserves.[4] At the same time, it sheds light on several aspects of EU consumer law.

While in competition law theories of harm are mainstream, like many sectorial mainstream ideas, they have not received extensive theoretical analysis. Arguably, a theory of harm is composed of three main layers:

i) the general doctrine of consumer harm – what is consumer harm?
ii) ways in which consumers are harmed – how does consumer harm happen?
iii) the case-specific scenarios of harm – how are consumers harmed in such and such context

In a first approximation, the three layers can be described as follows. The general doctrine of harm defines when consumer harm occurs, serving as the normative foundation of harm theory within a legal context. It outlines the types of harm, like high prices or limited choices, that laws seek to address, reflecting their protective goals. It establishes the standard for evaluating firms' conduct. The second layer of the theory of harm addresses the question of what causes harm, focusing on causation explanations. This layer reflects the prevailing knowledge and enforcement practices in a jurisdiction at a specific time. Empirical research plays a crucial role in shaping this layer, but it is also influenced by dominant institutional beliefs. In fact, the second layer of the theory of harm reflects the prevailing understanding and influences the current enforcement practices in a specific jurisdiction. While empirical research greatly informs this layer, it is also shaped by the prevalent institutional beliefs of the legal system in question.

This section articulates these elements and then discusses the main uses of this theoretical approach, namely both coherence-seeking and proposal of effectiveness-oriented interpretations of existing provisions as well as well as the proposal of new norms, rules, and principles.

4 For discussions, see Jules Stuyck, 'Book Review: Consumer Theories of Harm, An Economic Approach to Consumer Law Enforcement and Policy Making Paolo Siciliani, Christine Riefa and Harriet Gamper, Hart, Oxford, 2019', (2020) 9 Journal of European Consumer and Market Law 222; Fabrizio Esposito, 'Towards a General Theory of Harm for Consumer Law' (2021) 44 Journal of Consumer Policy 329. For an analysis along these lines, see also recently, Przemysław Pałka, 'Harmed While Anonymous: Beyond the Personal/Non-Personal Distinction in Data Governance' (2023) 2023 Technology and Regulation 22.

I. The elements of a theory of consumer harm and where to find them

1. What is harm?

The first layer, known as the general doctrine of harm, addresses the fundamental question of when consumer harm occurs. This aspect serves as the normative foundation of the theory of harm and establishes what constitutes legally relevant consumer harm in a certain legal context.[5] It provides a broad and theoretical explanation of the types of harm that the law aims to prevent or mitigate, such as high prices or restricted choices. This articulation of the general doctrine of harm refers to and can be inferred by looking at the protective objectives of the law. In essence, creating a general doctrine of harm involves specifying the normative standard against which firms' behavior is evaluated.

In civil law contexts, this first layer is deeply intertwined with a legal system's law of obligations, which determines what is a protected interest. It is then complemented by part of the law of contractual and tort liability specifying limitations to the recoverable damage. Finally, consumer law and sectorial legislation contribute to this activity. For example, the Air Passenger Rights Regulation grants a statutory right to compensation (Art 7) for the "serious trouble and inconvenience"[6] which can be increased under national law (Art 12).

An important issue of the theory of consumer harm approach is that, in its current development, the approach dismisses the idea that economic analysis of consumer transactions should solely prioritize maximizing overall or societal welfare, disregarding distribution between consumers and traders. Instead, it advocates for a consumer welfare standard.[7] There are compelling economic and legal justifications for favoring a consumer welfare standard in the analysis of market law. Therefore, the theory of harm approach should not raise concerns among consumer lawyers but should be embraced as an opportunity for enhanced interdisciplinary cooperation.

The concept of consumer sovereignty provides a sophisticated justification to the use of economic theory in the analysis of consumer-related

5 The expression 'legal context' is purposefully malleable. It can refer generically to EU consumer law, but also specifically to a first-instance court decision or to a specific piece of legislation (eg, the Italian Consumer Code). For a general discussion of the notion of legal context, see Uwe Kischel, *Comparative Law* (OUP 2019).

6 Recital 2.

7 Siciliani *et al*, n 3 above, 9.

issues that is, nevertheless, fitting with legal doctrine (contrary to most economic analyses of consumer law).[8] In a nutshell, consumer sovereignty is an equality norm that is supported by indirect reciprocity. The idea is that in a market economy, everyone is sovereign when acting as a consumer and subject of the consumers on the market where they act as producers. For example, a plumber is the subject of the recipients of their services, and the same plumber is then entitled to be sovereign at the supermarket, at the dentist's, etc. This idea has an impressive and mistreated history in economics; also, it fits well with the explicit structure of EU consumer policy, but also with the way in which EU consumer and antitrust law are interpreted and applied.

2. What causes harm?

The second layer relates to the question: 'What causes harm?' This component of the theory of harm relates to causation. It is made up of the set of accepted explanations for how harm happens. In competition law, this layer has been developed on the basis of economic analysis.[9] It comprises

8 Fabrizio Esposito, *Law and Economics United in Diversity* (Edward Elgar 2022) deals with the core theoretical and doctrinal foundations of the idea in EU antitrust and consumer law. This monograph is complemented by analyses that reinforce the account either by looking at sectorial legislation or engaging with specific theoretical perspectives. Fabrizio Esposito and Stefan Grundmann, 'Investor-Consumer or Overall Welfare: Searching for the Paradigm of Recent Reforms in Financial Services Contracts' (2017) *EUI Law Department Research Paper Series*, 2017/5; Fabrizio Esposito and Lucila de Almeida, 'A Shocking Truth for Law and Economics: The Internal Market For Electricity Explained With Consumer Welfare', in Klaus Mathis and Bruce Huber (eds), *Energy Law and Economics in Europe* (Springer 2018); Fabrizio Esposito and Lucila de Almeida, 'In Search of a Grand Theory of European Private Law: Social Justice, Access Justice, Societal Justice and Energy Markets', in Kai Purnhagen, Lucila de Almeida, Marta Gamito and Mateja Durovic (eds), *Transformation of Economic Law: In Honour of Hans-W Micklitz* (Hart Publishing 2019); Fabrizio Esposito and Giovanni Tuzet, 'Economic Consequence for Lawyers: Beyond the Jurisprudential Preface' (2020) 9 *Journal of Argumentation in Context* 368; Fabrizio Esposito, 'The Consumer Welfare Standard, Consumer Sovereignty, and Reciprocity: An Evolutionary Foundation for the Positive Economic Approach to Law that Actually Works', in Klaus Mathis and Avishalom Tor, *The Law and Economics of Justice* (Springer 2024); Fabrizio Esposito and Gianmaria Pessina, 'The Consumer Welfare Standard as an Endogenous Market Institution to Solve the Monopoly Prisoner's Dilemma', on file with the author.

9 See the literature referred to in footnote 2 for examples and discussions.

a typology of causal mechanisms that link certain market practices to consumer harm in certain contexts.

It should be noted that this second layer of the theory of harm expresses the received wisdom and characterizes the state of the art of enforcement in any given jurisdiction at any given point in time. This layer benefits immensely from empirical research but is also heavily influenced by the dominant institutional beliefs in a given legal context. At the same time, one should not forget that inappropriate legislative measures might well be part of the causes of harm.

The 'behavioural turn' which took place in the early 21st century illustrates all these points.[10] First, it was possible to challenge a received view about how consumers really behave, which was too optimistic. As part of that process, information-giving as a governance tool was heavily criticized. However, the critique led to a conscious focus on nudge in the US to offer a regulatory tool palatable to conservatives.[11] In the EU, instead, these studies lead to clear prohibitions (such as the one of pre-ticked boxes) and to proposals aimed at interpreting existing prohibitions in more incisive ways.[12]

Against this background, the theory of harm approach focuses predominantly on the limits of the market mechanism (the invisible hand) to deliver benefits to consumers. So far, the approach has not been developed in the direction of considerations about when certain legal measures are more or less likely to be desirable.

More precisely, the theory of harm approach distinguishes between two main types of traders and consumers: fair and unfair traders; sophisticated and naïve consumers. Traders are fair if they compete on the merits by offering the best possible deals to consumers; instead, they are unfair if they try to make a profit by exploiting "the well-known structural asymmetries

10 See, generally, Alberto Alemanno and Anne-Lise Sibony (eds), *Nudge and the Law: A European Perspective* (Hart Publishing 2015). See also Fabrizio Esposito, 'A Dismal Reality: Behavioural Analysis and Consumer Policy' (2017) 40 Journal of Consumer Policy 193 and Fabrizio Esposito, 'Conceptual Foundations for a European Consumer Law and Behavioural Sciences Scholarship', in Hans-Wolfgang Micklitz, Anne-Lise Sibony, Fabrizio Esposito (eds), Research Methods in Consumer Law (Edward Elgar 2018).

11 Richard H Thaler and Cass R Sunstein, 'Libertarian Paternalism' (2003) 93 The American Economic Review 175.

12 See, especially, Anne-Lise Sibony, 'Can EU Consumer Law Benefit from Behavioural Insights? An Analysis of the Unfair Practices Directive' (2014) 22 European Review of Private Law 901.

existing between consumers and traders".[13] Importantly, opting to compete based on merit is driven not primarily by altruism but by a profit-maximizing assessment.[14] As noted above, the approach is primarily focused on the motivation provided by the market mechanism, namely the invisible hand turning traders' self-interest into a means to foster consumers' interest.

At the same time, consumers can be divided into two groups that, for present purposes, can be named sophisticated and naïve consumers. This is a theoretical distinction that may or may not match that found in the UCPD of average and vulnerable consumers.[15] The distinction is functionally made on the basis of consumers' ability to identify a threat (cause of harm or vulnerability) in a certain choice architecture. By definition, sophisticated consumers can spot it, but naïve ones often cannot. More precisely, contractual attributes can be divided into three categories: search, experience and credence attributes. The idea is that ascertaining the true quality of these attributes is increasingly difficult. Naïve consumers often will not even check the quality of search attributes.

3. Scenarios of harm

Building on the content of the previous two layers, the theory of harm approach advocates examining specific market interactions using a framework of analytical constructs called 'scenarios of harm'. A scenario of harm consists of assumptions regarding the strategic interactions between traders and consumers, considering the varying levels of transparency associated with different transactions. Notably, scenarios of harm in their current formulation predominantly focus on the transaction as a homogenous entity.[16] However, as illustrated later in this chapter, the same framework can be used to analyze specific transactional attributes and, in particular, contract terms.

---

13 Fabrizio Esposito and Mateusz Grochowski, 'The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration' (2022) 18 European Review of Contract Law 1, 22.

14 Siciliani *et al*, n 3 above, 110 *et seq*.

15 Siciliani *et al*, n 3 above, 109 *et seq*. On this point, see, however, Esposito 2020, n 8, above.

16 See, for a more detailed analysis, Fabrizio Esposito and Anne-Lise Sibony, 'In Search of the Theory of Harm in EU Consumer Law: Lessons from the Consumer Fitness Check' in Klaus Mathis and Avishalom Tor (eds), *Consumer Law and Economics* (Springer International Publishing 2021), 255-259.

The arguably better account of the theory of harm approach, which is slightly different from the original one, includes four scenarios of harm: the benchmark, the lemon, *divide et impera*, the bottom. These scenarios are ordered from the less to the most concerning, especially from the perspective of the most vulnerable consumers.

Pragmatic reasons suggest refraining from elaborating on these four scenarios of harm for the moment. In fact, said information is not necessary to illustrate how the theory of harm approach can be used. At the same time, that information is best offered just before explaining how the scenarios shed light on issue pertaining to digital transactions, harm and vulnerability.

II. What a theory of harm can be used for

To discuss this topic, it is useful to briefly mention the experience of EU competition law, where the use of theories of harm increased as part of the more economic approach to law. In EU competition law, adopting a more economic approach has significantly benefited practice. It clarified that harming consumers is intrinsically problematic while harming competitors is only instrumentally so. It allowed enforcers to single out harmful conduct that would have been difficult to identify otherwise. In some occasions, it simplified the analysis of scenarios of harm for competition authorities by allowing courts to accept presumptions.[17]

As noted above, consumer law has not reached a stage of elaboration similar to competition law when it comes to conceptualizing harm or adopting a typology of conducts and market circumstances that lead to harm. For this reason, the first two layers of the theory need to be investigated further.[18] At the same time, the second part of this chapter illustrates that the scenarios of harm are sufficiently reliable to be applied in a variety of contexts.

17 Anne-Lise Sibony, 'Data and Arguments: Empirical Research in Consumer Law', in Hans-Wolfgang Micklitz, Anne-Lise Sibony, Fabrizio Esposito (eds), *Research Methods in Consumer Law* (Edward Elgar 2018)

18 Esposito and Sibony, n 16 above.

It has been persuasively argued that EU consumer law is directionless, necessitating a fundamental reconsideration.[19] This lack of clarity is especially problematic when determining how the law should adapt to digital markets. One primary challenge is the varying viewpoints of Member States, in particular concerning private law matters. Sometimes, ambiguities or non-specifics are intentionally adopted to achieve a directive consensus.

In this context, a more explicit expression of EU consumer law's protective intentions is beneficial. Firstly, it is not always apparent that the law's ultimate purpose is to protect consumers. A debate has emerged where some believe that the goal of market building has overshadowed the protection of vulnerable consumers. The Commission has actively sought to harmonize national consumer legislations to reduce business hurdles stemming from regulatory differences. As a result, EU consumer law seems more catered to empowered consumers who drive competition and market integration, sidelining the vulnerable population's needs.[20] Despite the advantages market integration offers (like increased choice and competitive pricing), some scholars argue it does not equate to genuine protection for the most vulnerable. In this regard, the proliferation of EU full harmonization directives and regulations is seen as particularly problematic, as it greatly limits Member States' power to intervene independently.[21] In terms of the theory of harm approach, this essentially means that the EU legislator assumes that the market is best understood as an instance of the scenarios of harm called benchmark and lemon, more than the more concerning *divide et impera* and bottom. In fact, the key difference between these two groups of scenarios of harm is the extent to which vulnerable consumers can benefit from the herd protection offered by the interaction between more autonomous consumers and traders.[22]

The second reason for more explicit articulation relates to regional and temporal variations. Different legal systems prioritize different consumer

19 Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking EU Consumer Law* (Routledge 2018).

20 Note that this view is different from the so-called instrumentalization critique, which holds that (private) law used to pursue ends which do not belong to it. Recently, Laura Burgers, Marija Bartl, and Chantal Mak, 'Introduction. The Evolving Concept of Private Law in Europe', Amsterdam Centre for Transformative private law Working Paper No. 2022-07. For an attempt to dispel this critique regarding the concept of allocative efficiency, see Fabrizio Esposito, 'What Can the Consumer Welfare Hypothesis Do for You? At Least Three Things…' (16 June 2023) *EU Law Live*.

21 Howells et alii, n 19 above.

22 See below, section 5.

benefits. One system might prioritize lower prices, even if it compromises other standards. In contrast, another might emphasize consumer rights like extended guarantees, potentially leading to higher prices and limited choices. These normative choices should be explicitly stated, aiding in comparisons between the EU's consumer law and those of other jurisdictions and enabling the assessment of its evolution and relevant criticisms.

Additionally, there is a practical need for well-defined theories of harmin EU consumer law. As penalties for consumer protection breaches could escalate to 4% of global turnover,[23] there will likely be more scrutiny of the reasoning behind infringement decisions. As the economic implications intensify, more litigation is expected, requiring clear guidance for both enforcement agencies and courts.

1. Reverse-engineering and coherence

Reverse-engineering legal reasoning involves inferring the objectives by examining how legal norms are justified, thereby gaining a deeper comprehension of them.

The purpose of reverse-engineering legal reasoning is an initial step in enhancing the legal system's design to enhance its effectiveness in achieving its intended objectives. In line with the social engineering paradigm, the focus during the reengineering phase is not on providing a normative assessment of policy objectives but rather on offering improved tools to attain given objectives. Naturally, after undergoing reverse engineering, the legal system may subsequently attract normative critiques aimed at altering its pursued policy goals, as discussed below. For the moment, the focus is on making explicit the relationship between the law's goals and the institutional design selected to achieve them.[24] This enhanced clarity can be used to perform one of the most traditional and ambitious doctrinal activities, namely investigating the coherence of the legal system. For example, one

23 Directive (EU) 2019/2161 of the European Parliament and of the Council 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 OJ L 328/7, Articles 1 and 3, introducting this penalty in the UCTD and UCPD, respectively.

24 For a clear and insightful analysis, see, Frans Leeuw and Hans Schmeets, *Empirical Legal Research: A Guidance Book for Lawyers, Legislators and Regulators* (Edward Elgar 2017).

may find that in a certain context, the institutional design assumes that the interest of less and more sophisticated consumers are aligned, but in a very similar one, the assumption is that their interests are misaligned. This incoherence is problematic and may lead to three outcomes: challenging the assumption that the two contexts are similar; arguing in favour of the former institutional design for both contexts; arguing in favour of the latter institutional design for both contexts.

To undertake the reverse engineering of legal reasoning, two essential components are required. First, there is a need for competing economic hypotheses to generate alternative explanations for the substance of legal reasoning. Second, a methodology for analyzing legal reasoning is necessary to determine which economic hypothesis aligns better with it.

In the process of reverse engineering legal reasoning, it is crucial to possess at least two competing hypotheses to assess their explanatory capacity. Additionally, these hypotheses can relate to either normative or empirical variables; for instance, the normative variable may involve the choice of a welfare standard, while the empirical one may concern the level of transaction costs.

The objective is to identify distinctions in the arguments constructed around one concept versus another. In the present context, the different theories of harm constitute the different hypotheses to be tested by looking at the reasoning justifying and applying certain concepts as legal concepts. As noted above, the theories assume that the normative goal is that of fostering the consumers' interests as much as possible.

Consider the controversy over dual-quality products that surfaced in Europe around 2017. This issue was so pressing that President Juncker addressed it in his State of the Union speech that year. Reacting to the discontent of numerous Eastern European leaders and European Parliament members, he emphasized that all consumers within the Union should be treated equally. He condemned the disparity where some European regions receive lower-quality food products than others, even when the branding and packaging are identical. The underlying concern, mainly shared by Central and Eastern European governments, is that Western European traders could potentially deceive their Central-Eastern European consumers by selling them inferior products.

The Modernisation Directive clarified that selling these dual-quality goods constitutes an unfair commercial practice. By definition, a product is considered dual quality if it has a "significantly different composition or characteristics" than another product but is marketed as the same.

The scenario of harm best associated with dual-quality goods sees Central-Eastern European consumers as targets of deceit. Western brands, perceived as premium, might reduce the quality of their products for this market. Local businesses would naturally resist such practices, while Western consumers could potentially benefit from indirect subsidization. Dual-quality products share traits of both lemon and *divide et impera* scenarios.[25] This is not surprising, in that Central-Eastern European traders face the problem typical of a lemon scenario, namely successfully showing the (higher) quality of their offers. At the same time, some Western traders are relying on geographical separations to implement the *divide et impera* strategy. By imposing a single-quality standard, the EU legislator managed to support Central-Eastern traders address the lemon problem and disincentivize the problematic *divide et impera* strategy relied upon by some Western traders.

The fact that the real-world issue straddles different archetypal harm scenarios should not discredit the framework. These scenarios are archetypes, not exhaustive categories. In particular, the real world is complex; so it might well be that different scenarios of harm coexist in the same market, as dual-quality goods illustrate. The significance of this framework is its ability to analytically (rather than emotionally) pinpoint the problematic aspects of dual-quality goods practices. A comprehensive understanding can then guide enforcement priorities and determine when a product truly exhibits dual quality.

To give another example, consider the transparency of core terms in consumer contracts. The CJEU currently reviews them only from the perspective of the average consumer.[26] If the interests of average and vulnerable consumers are aligned, then we are probably in the benchmark scenario, and this approach is justified. Yet, if we are in the *dividi et impera* scenario, vulnerable consumers are left to their own devices. When this is the case, a more robust, demanding, intrusive notion of transparency is justifiable because it is instrumental in protecting vulnerable consumers against unfair terms. This thicker notion of transparency requires that contract terms are transparent also for the vulnerable consumer. According to this thicker no-

25 Using the version of the framework we had in 2020, Anne-Lise Sibony and I concluded that the scenario was best understood as between the bottom and *divide et impera*. Probably, we underplayed the role of Central-Eastern traders back then.

26 The first case where this happened is Judgment of 30 April 2014, *Árpád Kásler and Hajnalka Káslerné Rábai v OTP Jelzálogbank Zrt*, C-26/13, ECLI:EU:C:2014:282, p. 74.

tion of transparency, Article 4(2) shields from the unfairness test only core terms that are transparent also for the vulnerable consumer. Conversely, Article 5 requires terms that are transparent also for the vulnerable consumer.

The thicker notion of transparency is beneficial to vulnerable consumers for the following reasons. Let us consider first the case where the complex offer is worse than the simple one – the hidden trap. The vulnerable consumer is likely to choose the complex offer. If this happens, under our proposed interpretation of Article 4(2), the core terms of the complex offer will not satisfy the transparency requirement. Consequently, these terms will have to be reviewed for their substantive fairness. Article 5 contributes to the overall deterrence of the UCTD by exposing the trader to additional legal sanctions.[27]

It is in the second case – the hidden gem – that Article 5 plays a pivotal role. In this case, the complex offer is better than the simple one. The vulnerable consumer is likely to opt for the simple offer, even if less advantageous. Against this background, a thicker notion of transparency in Article 4(2) will not do much to help the vulnerable consumer. In fact, by assumption, the simple offer will also be transparent according to the thicker notion of transparency. Consequently, vulnerable consumers are prone to choose simpler and less advantageous offers, to their detriment. To benefit the vulnerable consumer, the UCTD should motivate traders to increase the transparency also of the complex offer. When both offers become transparent, the vulnerable consumer should join the average one in preferring the complex offer. However, Article 4(2) cannot be used for this purpose. The reason is simply that the complex offer has not been accepted by the consumer: the consumer has chosen the simple offer. Accordingly, only the terms of the simple offer can be reviewed pursuant to Article 4(2).

It follows that it is necessary to look elsewhere to find a deterrence mechanism against the drafting of complex but advantageous offers marketed in tandem with simpler and less advantageous ones. Article 5 of the UCTD can be used to this end. Since this provision introduces a general obligation to draft transparent terms, it can also be used against complex but advantageous offers (within the meaning of these terms as used in the

27 Even after the adoption of the Modernization Directive, Member States enjoy wide discretion in establishing the legal consequences of violating Article 5. On the matter, see eg Vanessa Mak, *Legal Pluralism in European Contract Law* (OUP 2020) 157-159; Paolisa Nebbia, *Unfair Contract Terms in European Law* (Hart 2007).

previous section). It should be remembered that the CJEU's case law on sanctions in EU consumer law leaves ample room for national legal systems to design sanctions.[28]

Only pecuniary sanctions (damages and/or fines) would be easy to apply to the situation under scrutiny. In this situation, the trader is sanctioned for the lack of transparency of the terms of a contract that ultimately the vulnerable consumer has chosen not to enter into. Under the current scheme of the UCTD, it seems hard to apply remedies such as termination, rescission, nullity, or revision. All these remedies presuppose that the opaque term is part of the contract that is binding the consumer. However, in the situation under scrutiny, this is not the case.

2. Interpretation, integration and policy proposals

Theories of harm can be transformative in the legal system. In fact, one can use them to organize the ideas supporting the claim that a certain provision needs to be interpreted in a certain way or, more explicitly, to recommend a legislative reform. I provide three examples to illustrate this point: the right to transparent terms for vulnerable consumers; the right to know the impersonal price and how much the price was personalized; a positive duty of care towards consumers.

As anticipated, reverse-engineering is also useful for a more critical investigation of legal materials, as illustrated by the plea for reconsidering the view that the transparency standard of contract terms in the Unfair Contract Terms Directive should always be only that of the average consumer.[29]

As anticipated, sometimes a more robust interpretation of transparency requirements in the Unfair Contract Terms Directive is necessary to safeguard vulnerable consumers from unfair terms. The advocated "thicker" transparency ensures that contractual terms are clear even for such vulnerable consumers. Under this understanding, Article 4(2) of the UCTD would only protect core terms from an unfairness review if they are trans-

28 See, recently, Judgment of 10 June 2021, *Ultimo Portfolio Investment*, C-303/20, ECLI:EU:C:2021:479.

29 Esposito and Grochowski, n 12 above; Fabrizio Esposito, Leonor Gambôa Machado and Mateusz Grochowski, 'Será que o Direito Português confere melhor proteção aos consumidores vulneráveis que o Direito da União Europeia no contexto de cláusulas abusivas em contratos de consumo? Uma análise jurídica e económica' (2022) 6 Católica Law Review 83.

parent to the vulnerable consumer. Additionally, Article 5 would necessitate this higher degree of transparency.

The importance of this enhanced transparency is evident in two contexts, called the Hidden Gem and the Hidden Trap. In the Hidden Trap, a complex offer is less beneficial than a simpler one. Vulnerable consumers, not fully grasping the intricacies, might (even randomly) opt for the complex offer. Notably, it would be economically rational in competitive markets to make the simpler one more expensive, which shows that competition will not solve the problem.[30] Under the proposed transparency, the core terms of this complex offer will meet the transparency criteria and will be scrutinized for fairness. Article 5 further ensures trader accountability by introducing additional legal consequences.

In the Hidden Gem, the complex offer is more beneficial than the simple one. Despite its advantages, vulnerable consumers might go for the simpler offer due to its apparent clarity and possibly lower price.[31] The enhanced transparency in Article 4(2) has a limited impact here, as even with this stringent transparency measure, the simpler offer would still appear clear. Hence, vulnerable consumers might still choose the less beneficial offer. For the UCTD to truly benefit vulnerable consumers, it should encourage traders to make even complex offers transparent. However, since the consumer has chosen the simple offer, only its terms can be reviewed under Article 4(2).

This necessitates an alternative deterrent against offering complex yet beneficial terms alongside simpler, less beneficial ones. Article 5 can play this role. Given its emphasis on drafting transparent terms, it can address even complex but advantageous offers. The CJEU's case law provides flexibility in designing sanctions within the EU consumer law framework.

A core element of this analysis is showing that the *communis opinio* on how the UCTD protects consumers from unfair terms rests on the premise that core unfair terms is best understood as an instance of the benchmark scenario. However, the focus on the Hidden Traps and Gems allows us to show that, at least in those circumstances, the situation is best understood as a more alarming scenario, namely *divide et impera*. On these premises,

30 In legal scholarship, see Oren Bar-Gill, *Seduction by Contract : Law, Economics, and Psychology in Consumer Markets* (OUP 2012).

31 For the same reason, making the more complex offer cheaper than the simpler one in the Hidden Trap: competitive pressure.

a more intrusive (for traders) and protective (for consumers) interpretation of Article 4(2) and 5 UCTD are proposed.

Second, consider the provision introduced by the Modernization Directive stating that consumers have the right "where applicable, to know that the price was personalised on the basis of automated decision-making". This provision has been typically interpreted according to its plain meaning, thereby granting consumers the right to know that the price was personalized.[32]

Arguably, this right is not effective enough and stronger interventions are needed, starting with the right to know how much the price was personalized.[33] Why? For current purposes, it is sufficient to anticipate that exploitative price personalization is likely an instance of the *divide et impera* scenario, if not the bottom scenario. Against this background, the right to know that the price was personalized is ineffective. In fact, merely knowing that the price was personalized, without further information of the outcome or consequences of said personalization is not useful to the consumer. This is especially true for those (I suspect the overwhelming majority) who do not infer from the fact that the trader did not frame the personalization as an explicit discount that the trader is most probably offering a personalized (and exploitative) surcharge. These consumers need to know how much the price was personalized in comparison to the impersonal price. Note that a plausible interpretation of the GDPR leads to the conclusion that consumers at least have the right to be offered an impersonal price.[34] This is less than, but the logical precondition of, the right to know how much the price was personalized. Thanks to the GDPR, consumers can resist the processing of their data to personalized the price, thereby being offered an

32 See, IPSOS, London Economics, Deloitte, *Consumer Market Study on Online Market Segmentation through Personalised Pricing/Offers in the European Union* (2018); Alan Sears, "The Limits of Online Price Discrimination in Europe" (2020) 21 Science andTechnology Law Review 1; Sebastião Barros Valle, "The Omnibus Directive and Online Price Personalization: A Mere Duty toInform?" (2020) European Journal of Privacy Law & Technologies; Competition & Market Authority (CMA), Algorithms: How They Can Reduce Competition and Harm Consumers; Hans-Wolfgang Micklitz, Peter Rott, Natali Helberger, O Lynskey, Marijn Sax, Joanna Strycharz, *Structural Asymmetries in Digital Consumer Markets* (BEUC 2021); OECD, *Disclosure about Personalised Pricing on Consumers. Results from a Lab Experiment inIreland and Chile* (OECD 2021).

33 Fabrizio Esposito, "Making Personalised Prices Pro-Competitive and Pro-Consumers" (2020) 2/2020 *CeDIE Working Paper*.

34 Fabrizio Esposito, 'The GDPR Enshrines the Right to the Impersonal Price' (2022) 45 Computer Law & Security Review 105660.

impersonal price. The right to know how much the price was personalized means that the information about the impersonal price is given together with the one about the personalized price.

The seminal book *Consumer Theories of Harm* offers a wealth of examples of situations in which consumers are expectably suffering a suboptimal level of harm, in situations as diverse as retail energy markets, bank current and savings account, compensation and seating in the airline industry and fertility add-ons. On these grounds, the authors advance a convincing argument supporting the view that moving away from a negative duty not to trade unfairly and towards a positive duty to trade fairly is necessary.[35]

C. Four scenarios of consumer harm

I. A first approximation

It is possible to identify at least four archetypical scenarios of harm: the bottom, the lemon, *divide et impera*, and the benchmark. The bottom is the scenario where there are not enough average consumers to police the quality of traders' offers. Accordingly, traders do not compete on the merits and focus on exploiting consumers. The lemon is the scenario where traders struggle to compete on the merits because they face significant challenges in signalling the quality of their offers and thereby distinguishing themselves from profiteers. *Divide et impera* is the scenario where the interests of the average and vulnerable consumers could be aligned but have been artificially disconnected by the trader.

Finally, in the benchmark scenario, the interests of the average and vulnerable consumers are aligned. The average consumers are offering a form of herd protection to the vulnerable consumers. In other words, average consumers operate on the market by choosing traders competing on the merits. By doing so, they help these traders to succeed on the market by sidelining the profiteers. In this context, the vulnerable consumers benefit from the exercise of their power of choice by the average consumers.

The book *Consumer Theories of Harm* introduced another scenario called 'the subsidy'.[36] In this scenario, sophisticated consumers benefit from

35 Siciliani et alii, n 3, above, 179-208.
36 Siciliani et alii, n 3, above.

a consumer right or power, but that very same right or power is useless for the less sophisticated consumer (typically because it is too complex to exercise). The scenario does not seem well-designed for the following reason. Even if a consumer does not exercise the right to withdraw, the same consumer could benefit from other consumers putting pressure on the trader by exercising that right (and leaving also a negative review). Generalizing, the fact that some consumers do not exercise a right does not mean they are merely subsidizing other consumers as long as the interests of the two groups are aligned and the exercise of the right by one group is also beneficial to the other group.[37] The central concern seems whether the trader successfully eliminates the herd protection naïve consumers enjoy because of sophisticated consumers' behaviour. Hence, it appears appropriate to substitute the subsidy scenario with *divide et impera*.

II. The scenarios in more detail

1. The benchmark

In the benchmark scenario, fair and unfair firms struggle to distinguish between sophisticated and naïve consumers.[38] Accordingly, sophisticated consumers offer a degree of protection to the naïve ones. This protection is stronger, the higher the number of sophisticated consumers, and the more homogeneous the interests of the two groups are. The scenario covers situations of price obfuscation and evaluation inflation, in which the unfair firm tries to downgrade search attributes into latent credence attributes, thereby reducing competitive pressure on them. In these cases, the unfair firm attempts to obscure search attributes, turning them into less visible features, thus diminishing the competitive pressure they face.

37 See, more extensively on this, Fabrizio Esposito, Antonio Davola, Mateusz Grochowski, '
Price Personalization vs. Contract Terms Personalization', in Fabrizio Esposito and Mateusz Grochowski (eds), *Cambridge Handbook of Algorithmic Price Personalization and the Law* (CUP forthcoming).

38 Siciliani et alii, n 3, above, 126.

Note that this scenario is called the benchmark because it represents the best non-ideal set of circumstances:[39] the appropriate legal intervention will empower sophisticated consumers to exercise enough pressure on traders so that fair trading behaviour will become common, to the benefit also of naïve consumers whose interests, as noted, are aligned with the sophisticated consumers.

2. The lemon

In the lemon scenario, named after Akerlof's market for lemons model,[40] fair traders struggle to effectively signal their offers' quality to consumers, distinguishing them from the unfair traders' offers. This is thus an unstable scenario. When fair traders fail to solve this quality-signaling problem, both fair and sophisticated consumers exit the market, which then collapses in the bottom scenario.

Good durability and competence of a service provider are typical examples of this issue. The law intervenes with mandatory and voluntary durability warranties and guarantees[41] and minimum quality standards, such as the bar exam.

3. *Divide et impera*

In the *divide et impera* scenario, the interests of sophisticated and naïve consumers are artificially misaligned. 'Artificially' here stresses that, but for some trader's conduct, the interests of sophisticated and naïve consumers would be aligned. Note that the conduct does not necessarily be one that explicitly segregates consumers into different groups. Self-selection mechanisms allowing consumers to separate themselves actively are sufficient.

---

39 On the distinction between ideal and non-ideal theories in relation to market allocations, see Joseph Heath, *Morality, Competition, and the Firm: The Market Failures Approach to Business Ethics* (OUP 2014).

40 George Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 The Quarterly Journal of Economics 488. On which, see Stefan Grundmann, 'Knowledge and Information', in Stefan Grundmann, Hans-Wolfgang Micklitz & Moritz Renner (eds), *New Private Law Theory: A Pluralist Approach* (CUP 2021), 241-246.

41 See, for example, Artt. 5-9 and Art. 17, Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC OJ L 136/28.

4. The bottom

The bottom is the worst possible scenario. In this scenario, traders' offers are "worthless or of little value".[42] This scenario is populated only by unfair firms who exploit naïve consumers and their vulnerabilities. In other words, there is no fair firm operating in this market, and sophisticated consumers know this and stay away. Pyramid and Ponzi schemes and fake lottery prices are good examples of this. Glamorous Ponzi schemes like the one orchestrated by Bernie Madoff (20 billion USD) remind us that also normally sophisticated consumers can 'hit the bottom'.

5. On the relationship between the scenarios

Let us elaborate on the relationship between these scenarios. The benchmark scenario is the most favourable one for all consumers, while the bottom is the least favorable for the vulnerable consumers. The lemon scenario is volatile: if traders (or the legal framework) effectively address the signaling issue, consumers' situation improves to the benchmark scenario; if not, it deteriorates to the bottom scenario.

Divide et impera is, in a way, the most dangerous scenario, especially in the digital environment. Two features of the digital economy make it particularly relevant. First, the ability to create granular distinctions is useful to create offers that will have different degrees of appeal for sophisticated and naïve consumers, thereby misaligning their interests. At the same time, digital offering space is way more abundant than shelves in aisles, so granular offerings become also more common.

Ultimately, the key question is whether empowering sophisticated consumers (in particular, via information disclosure and the right to withdraw) will be enough to foster all consumers' interest in the market, or not. When that is not the case, more intrusive forms of intervention are required.[43] In the benchmark, this seems within reach. So is in the lemon scenario if the quality signal problem is solved. Note that solving the quality problem may require mandatory protective interventions such as minimum standards to expel scammers from the market. The extensive systems of market surveil-

42 Siciliani et alii, n 3, above, 112.

43 Esposito 2017, n 10, above and Fabrizio Esposito, *Law and Economics United in Diversity: Towards a Synthesis for the 21st Century* (Edward Elgar 2022), 175-180.

lance[44] in place to ensure that goods, but also food, drugs, etc, are safe show how extensive the EU protective net is—and by implication, how unfair it is to keep lamenting that the information paradigm dominates the EU governance of consumer transactions.

On these grounds, it is now possible to discuss three concerning situations that can be illuminated by the theories of harm approach.

D. Divide et impera *in digital marketplaces*

The first example is the fact that in online marketplaces, space is more abundant than shelves in the physical world. It follows that traders can make way more offers for similar products while introducing a significant degree of variation in the offers.[45]

I. Shopping between hidden traps and hidden gems as the new normal?

Traders frequently provide two versions of a product or service: a straightforward version and a more intricate one. While the sophisticated consumer grasps both, the naive consumer only understands the simple version. Such dual offerings are common, with examples including basic and premium internet plans. As per Articles 4(2) and 5 UCTD, traders are legally secure as long as both offers are deemed clear for the average consumer. However, this overlooks the vulnerable consumers who cannot discern the intricate offer's nuances, leaving them susceptible to exploitation.

To delve deeper, consider two contrasting scenarios. In one, the straightforward version is superior, while the intricate version has a concealed disadvantage ("Hidden Trap"). In the other scenario, the intricate offer is better, concealing a benefit ("Hidden Gem").

Considering the Hidden Trap scenario, the complex offer might involve unexpected costs, like a deductible for accidents. While some research has explored why consumers fall for these traps, the protective role of the sophisticated consumer towards the naïve has not attracted much attention. In such a context, the average consumer recognizes the simpler offer's better value and opts for it. But this choice does not deter traders from presenting

44 See, generally, Pieter Van Cleynenbreugel, *Market Supervision in the European Union: Integrated Administration in Constitutional Context* (Brill 2014).

45 See, more extensively, Esposito and Grochowski, n 13, above.

both versions. The vulnerable consumer, unable to identify the trap in the complex offer and likely enticed by a lower price, may be drawn to it. Under current interpretations of Articles 4(2) and 5 UCTD, this is lawful, even if it exploits vulnerable consumers.

In the Hidden Gem scenario, the complex offer might bundle a product with an additional beneficial service at a competitive price, such as car rentals with insurance. Is this any better for the vulnerable consumer? It isn't. Like the prior situation, average consumers discern the complex offer's superiority, finding the gem. In contrast, vulnerable consumers may see the straightforward, less beneficial offer as better, missing out on the concealed advantage. Again, the prevalent interpretation of Articles 4(2) and 5 UCTD does not afford ample protection to consumers.

In both contexts, whether facing a hidden trap or hidden gem, naïve consumers remain susceptible to harm. Sophisticated consumers' choices do not discourage traders from maintaining both offers, leaving the naïve ones at a consistent disadvantage.

II. The naïve consumers' right to transparent contract terms

What can be done for the naïve consumers? The assumption that sophisticated consumers will adequately protect the naïve ones is at the core of the rationale behind the *communis opinio*. The same idea is also at the core of the benchmark scenario. Accordingly, the benchmark scenario can be used to describe in more detail the rationale behind the *communis opinio*.

Using the conceptual apparatus developed by the theory of harm approach, our claims can be reformulated as follows. The *communis opinio* is wrong in considering that average consumers will protect the interests of the vulnerable ones regarding core terms; in other words, the *communis opinio* is wrong in considering core contract terms as an instance of the benchmark scenario. In some situations, at least, traders can use self-selection mechanisms based on opacity to 'divide and conquer' consumers. When this happens, naïve consumers find themselves in the bottom scenario, not in the benchmark one. This means that consumers are living in the *divide et impera* scenario. Let us see why.

As currently understood, Articles 4(2) and 5 of the Unfair Contract Terms Directive presuppose that core contractual terms fall within the last scenario – the benchmark. In other words, Articles 4(2) and 5 are based

on the assumption that naïve consumers are adequately protected by the behavior of the sophisticated consumer in relation to core terms.

This conclusion follows directly from the idea that it is sufficient to review the transparency of core terms from the sophisticated consumer's perspective. The reasoning is as follows: traders who want to attract sophisticated consumers have to offer transparent and attractive terms. Thus, also naïve consumers benefit from the traders' fear of losing business opportunities with sophisticated consumers. Indeed, the mainstream economic analysis of consumer law supports this view, especially in relation to core terms.[46] This analytical framework has been used to analyze the distinction between core and ancillary terms in UCTD.[47]

A partial solution requires that core terms must also be transparent from the perspective of naïve consumers. When this is not the case, then it will be possible for the judge to analyze the substantive fairness of the price-quality ratio, taking into consideration the existence of the hidden gem and hidden trap. In an individual transaction, the presence of the hidden trap will have more straightforward consequences since the naïve consumer has selected the contract with such terms. More problematic is the situation of the hidden gem, since the consumer, in this case, has opted to enter into the simple contract. At least, even in such cases, one can complain that the trader violated Article 5 UCTD in hiding the gem. Admittedly, however, the benefit for the consumer will be limited. This is not surprising, considering that this situation has failed to receive any attention until recently.

E. Hyper-engaging practices pulling us to the bottom

Content-sharing platforms are one of the most significant socio-economic developments in digital environments. Why do they work so well? Because they hook users by design, which makes them a problematic commercial

46 Broad survey in Esposito 2017, n 10, above. Recently, Ann-Sophie Vandenberghe, 'The Law on Unfair Terms in Standard Form Contracts in Europe', in Klaus Mathis and AvishalomTor (eds), *Consumer Law and Economics* (Springer 2020), 126-127 and Esposito and Grochowski, n 13, above.

47 Matteo Dellacasa, 'Judicial Review of "Core Terms" in Consumer Contracts: Defining the Limits' (2015) 11 *European Review of Contract Law* 152; Fernando Gómez Pomar, 'Characterizing Economic and Legal Approaches to the Regulation of Market Interactions', in Peter Cserne and Fabrizio Esposito (eds), *Economics in Legal Reasoning* (Palgrave 2020) 63.

practice. They do it because they are the clearest example of hyper-engaging practices (H-EPs).[48]

I. Hyper-engaging practices: capturing and retaining user attention

Hyper-engaging practices are tactics used online, especially by content-sharing platforms, to capture and retain user attention. These strategies focus on exploiting human attentional limitations and reinforcing certain behaviours to make using a service a habitl. H-EPs tap into the limited attentional resources of humans. Common manifestations include infinite scrolling, autoplay, push notifications, emojis, disappearing stories, follower counts, and more. By targeting human attention, they often compromise rational decision-making.

H-EPs have two main components. The first is the use of adaptive algorithms to personalize content for users. Algorithms analyze past interactions and adjust future content, providing a sense of reward. The second is the use of behavioural reinforcement techniques, which match closely the Dopamine System. Dopamine, a hormone, plays a key role in habit formation. In fact, the activation of the dopaminergic system encourages the repetition of actions that previously led to rewards. The dopamine cycle, comprising stages of wanting, seeking, anticipating, triggering, and rewarding, is essential to understanding repeated engagement with online platforms.

The so-called Hook Model well illustrates the above.[49] The Hook Model is a major blueprint for creating habit-forming products: it includes triggers, actions, variable rewards, and investments. This model closely mimics the dopamine cycle, leading to habitual use of platforms. Content-sharing platforms like YouTube, Facebook, and TikTok clearly resemble the Hook Model. Features like likes, shares, comments, etc., serve as variable rewards, while the scarcity of certain content (like stories) and features like infinite scrolling keep users engaged.

Hyper-engaging practices raise concerns generally in terms of manipulation, but for some users, the problem can degenerate into addiction. H-EPs are manipulative by nature: they can direct user behaviour without the

48 Fabrizio Esposito and Thaís Maciel Cathoud Ferreira, 'Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns' (2024) *European Journal of Risk Regulation* 1.

49 Nir Eyal, *Hooked: How to Build Habit-Forming Products* (Portfolio 2014).

user's awareness, compromising autonomous decision-making. This occurs as platforms exploit cognitive biases in users, pushing them to spend more time online. Did it ever happen to you to open one of these platforms 'to give a quick look' and then 30+ minutes had passed? That is the first problem I am referring to.

Some users are not so lucky, and for them, the habit degenerates into internet addiction, which results in negative physical, mental, and social effects. The continuous dopamine cycles make offline life less gratifying.

Hyper-engaging practices are a form of nudge. In fact, a 'nudge' alters behavior through certain aspects of choice architecture that are not relevant from a rational choice perspective.[50] When big data analytics play into nudges, they become 'hypernudges'.[51] Hence, H-EPs can be defined as a type of hypernudge, where the digital interface influences users to spend more time online. H-EPs are also dark patterns. Dark patterns are practices that distort or prevent users from making informed choices.[52] H-EPs can be seen as a subset of dark patterns due to their manipulative nature and impact on behaviour. Unsurprisingly, dark patterns often overlap with hypernudges as they both affect user behaviour using big data.

The scenario of harm that most closely resembles the use of hyper-engaging practices is the lemon, but with a clear negative trend toward the bottom. In fact, consumers are at the mercy of unscrupulous traders who design their service to make it, in essence, addictive. Moreover, it is difficult to predetermine which consumers will be prey of hyper-engaging practices.

At the same time, content-sharing platforms can be useful and meaningful to people's lives in many ways. This is true even if one focuses more specifically on social media.[53] Accordingly, one should not ignore that content-sharing platforms can and potentially could be very valuable to their users. Accordingly, it seems that these services are facing the quality problem characteristic of the lemon scenario so regulatory intervention could be pretty effective in orienting competitive pressure towards truly value-creating service innovation.

---

50 See, for a discussion, Esposito 2018, n 10, above.

51 Karen Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design' (2017) 20 Information, Communication & Society 118.

52 Broad survey in Jamie Luguri and Lior Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13 *Journal of Legal Analysis* 43.

53 See, however, Jaron Lanier, *Ten Arguments For Deleting Your Social Media Accounts Right Now* (Henry Holt and Co. 2018).

II. Hyper-engaging practices plausibly violate the Unfair Commercial Practices Directive

Already the Unfair Commercial Practices Directive (UCPD)[54] can be used to help traders in industries where H-EPs are and could be used pervasively to combat said practice. In fact, the UCPD aims to safeguard consumers from, among others, manipulative commercial practices that might distort their decision-making processes. Hyper-engaging practices are indeed likely to infringe upon the UCPD.

As seen, H-EPs are characterized by their ability to engage users by exploiting cognitive vulnerabilities and enticing users to make decisions that serve the platform's financial interests. The power of these practices lies in their subtlety; in fact, they often operate in an organic way, with users perceiving their engagement decisions as a product of free will.

For a practice to be deemed unfair under the UCPD, it must, first of all, satisfy the 'transactional decision test': the practice should cause the average consumer to make a transactional decision that they would not have taken otherwise. The Court of Justice of the European Union (CJEU) has interpreted this concept broadly, suggesting it encompasses not just purchasing decisions, but any decisions related to them.[55] Hence, any strategy designed to capture consumer attention falls within the UCPD's purview. Given H-EPs' manipulation of user behaviour for financial gain, they potentially breach this test. This is confirmed by the fact that the use of H-EPs is advised in popular marketing literature.[56]

Admittedly, in the digital environment, it is challenging to demonstrate the precise impact of H-EPs on user behaviour empirically. However, evidence from the literature and other studies on online manipulation

54 Directive 2005/29/EC of the European Parliament and of the Council 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 OJ L 149/22.

55 See Judgment of 19 December 2013, *Trento Sviluppo srl, Centrale Adriatica Soc. Coop. Arl v Autorità Garante della Concorrenza e del Mercato*, C-281/12, ECLI:EU:C:2013:859.

56 Eyal, n 49, above; Richard Shotton, *The Choice Factory: 25 Behavioural Biases that Influence What We Buy* (Harrington House 2018); A K Pradeep, *The Buying Brain: Secrets for Selling to the Subconscious Mind* (Wiley 2021).

corroborates the claim that H-EPs exploit cognitive vulnerabilities.[57] This manipulation often leads to heightened user engagement, causing decisions which might not have been made in the absence of these manipulative cues.

While H-EPs might seem to be misleading, they are best understood as aggressive commercial practices. Misleading practices revolve around withholding or distorting information. H-EPs, however, are immune to information provision. Their potency is not in the concealment of information but in the very architecture of their design. They represent a more profound threat to consumers, surpassing mere misleading tactics.

Articles 8 and 9 UCPD prohibit aggressive commercial practices. These are practices that employ, among others, undue influence, which impairs consumers' freedom of choice, leading them to decisions they would not ordinarily make. Given H-EPs' manipulative nature, they fit well within this description.

In fact, the UCPD defines undue influence as a situation where a trader exploits a position of power over a consumer, pressuring them and limiting their ability to make informed decisions. Notably, the CJEU has shown flexibility in interpreting undue influence, considering not just explicit but also implicit, more subtle forms of pressure.[58]

H-EPs are successful due to their ability to guide user decisions stealthily. By design, they direct attention and influence user choices, often below conscious awareness. In the broader framework of the UCPD, and particularly given the mandate to be future-proof, these manipulative practices should be interpreted as exerting undue influence. This view is bolstered by

57 See, for example, World Health Organization, *Public Health Implications of Excessive Use of the Internet, Computers, Smartphones and Similar Electronic Devices: Meeting Report, Main Meeting Hall, Foundation for Promotion of Cancer Research, National Cancer Research Centre, Tokyo, Japan, 27-29 August 2014* (World Health Organization 2015) <https://apps.who.int/iris/handle/10665/184264> accessed 5 June 2023; Patti Valkenburg, Adrien Meier and Ine Beyens, 'Social Media Use and Its Impact on Adolescent Mental Health: An Umbrella Review of the Evidence' (2022) 44 Current Opinion in Psychology 58.

58 Judgment of 18 October 2012, *Purely Creative Ltd and Others v Office of Fair Trading*, C-428/11, ECLI:EU:C:2012:651; Judgment of 13 September 2018, *Autorità Garante della Concorrenza e del Mercato v Wind Tre SpA and Vodafone Italia SpA*, C-54/17, ECLI:EU:C:2018:710; Judgment of 12 June 2019, *Prezes Urzędu Ochrony Konkurencji i Konsumentów v Orange Polska*, C-628/17, ECLI:EU:C:2019:480.

the UCPD Guidelines and other legal literature that links undue influence with manipulative tactics.[59]

In case the above claim is rejected, H-EPs shall be analyzed through the lenses of Article 5 UCPD, the general prohibition designed to target unfair commercial practices not covered by other UCPD provisions. Pursuant to this general prohibition, a practice is deemed unfair if it goes against professional diligence and can notably alter the average consumer's economic behaviour. Despite the prevalence of H-EPs, they are often manipulative, violating the principles of good faith and fair dealing. In particular, employing H-EPs that compromise users' autonomy is in breach of professional diligence. The UCPD's Article 5(2) implements the transactional decision test, which relates to H-EPs' influence on consumer behaviour. Even if H-EPs are not labelled aggressive, they should be classified as unfair practices under Article 5(2) UCPD, given their propensity to steer consumer behaviour.

In summary, the UCPD can prohibit H-EPs. Even if these tactics were not foreseen when the directive was enacted, UCPD's provisions can be construed to ban H-EPs, categorizing their deployment as an unfair practice.

F. Divide et impera *by way of price personalization*

Price personalization has been receiving a significant among of attention by academic policy-makers and stakeholders in the recent years. Indeed, it is a topic of great complexity from normative, institutional, descriptive, and methodological perspectives (especially from an interdisciplinary viewpoint).[60]

This complexity is well-illustrated by the change of position by BEUC, the European Consumer Organization, on the matter. During the legislative process leading to the Modernization Directive, BEUC claimed consumers needed 'blunt' transparency about the fact that a price is personalized;[61]

59 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 [2021] OJ C526/1, 100-104.

60 See, broad survey in Esposito and Grochowski forthcoming, n 37, above.

61 BEUC, *Proposal for a Better Enforcement and Modernisation of EU Consumer Protection Rules – "Omnibus Directive". The BEUC View* (BEUC 2018).

the European Parliament amended the directive's text to that effect. In the summer of 2023, BEUC proposed to ban price personalization.[62]

This U-turn is problematic in two respects. The first is methodological. Not much justification was provided a few years ago, while the more recent analysis fails to engage with the relevant literature. The second is that there are substantive reasons that while the 'blunt' transparency position is not enough, the 'blunt' prohibition errs in the opposite direction.

The theory of harm approach helps to articulate these points.

I. The economic preconditions of exploitative price personalization

Price personalization is not necessarily detrimental to consumers.[63] In fact, price personalization can be understood as a way to foster 'spatial competition'. It is a fact that offers can be of different quality. This difference can be 'vertical', for example, between budget and premium versions of a good or service; or they can be 'horizontal', so that different people will prefer different offers. Food, beverages and clothing are sectors were both distinctions coexist: Coca vs Pepsi (horizontal); Ferrari vs Twingo (vertical); pizza vs sushi (horizontal); Rolex vs Casio (vertical); etc.

The point is that, as discussed below, price personalization can be exploitative of consumers; but it can also benefit them. First, it can increase access. If a consumer is willing to pay below market price but above cost, it will be profitable to the trader to offer a personalized discount to that person. Second, it can stimulate competition, especially between horizontally-differentiated offers. The intuition is that a discount could motivate a loyal consumer of product A to try out product B. Of course, algorithmic price personalization also poses threats to the competitive process.[64] But the point is that this is complex business practice with lights and darks and should be analyzed and governed with nuance.

62 BEUC, *Each Consumer a Separate Market? - BEUC Position Paper on Personalised Pricing* (BEUC 2023).

63 See, generally, Office for Fair Trading (OFT), *The Economics of Online Personalised Pricing* (OFT 2013); OECD, *Personalized Pricing inthe Digital Era* (OECD 2018); Esposito 2020, n 33, above; Esposito and Grochowski forthcoming, n 37, above.

64 See, Christopher Leslie, "Predatory Pricing Algorithms" (2023) 98 *New York University Law Review* 49 and Thomas Cheng and Julian Nowag, "Algorithmic Predation and Exclusion" (2023) 25(1) *University of Pennsylvania Journal of Business Law* 41.

Let us focus on the use of price personalization to extract rents from consumers. There is widespread agreement among economists that traders can use algorithmic decision-making to increase prices to specific (groups of) consumers under the following conditions: profiling capacity; some degree of bargaining power; obstacles to arbitrage.[65]

The first requirement is that traders have an increased ability to understand how much consumers are willing to pay for a product or service.[66] The second is some degree of bargaining power.[67] This bargaining power can originate in the market structure and the lack of competitive pressure, or more situational elements. Within the elusive notion of situational bargaining power,[68] obfuscation practices have received particular attention.[69] An obfuscation practice hides behind a veil of complexity (linguistic or otherwise) the risks the consumer is exposed to; obfuscation limits the decisional ability of the consumer. For example, a credit agreement where the interest rate is calculated in national currency, but the credit is issued and then reimbursed in a foreign currency with the implication of the exchange rate applied by the lender makes the consumer pay the lender twice: first by paying the interest rate; second by paying the mark-up on the exchange rate applied by the lender.[70]

65 OECD, n 63, above and OFT, n 63, above.

66 See, generally, Katsov, Ilya, *Introduction to Algorithmic Marketing: Artificial Intelligence for Marketing Operations* (Sunnyvale 2017).

67 See OECD, n 63, above and OFT, n 63, above. See also Juan-José Ganuza and Gerard Llobet, 'Personalized Prices in the Digital Economy', in Juan-José Gauza and Gerard Lobert (eds), *Economic Analysis of the Digital Revolution* (FUNCAS 2018).

68 Michael Trebilcock, *The Limits of Freedom of Contract* (Harvard University Press 1991).

69 Xavier Gabaix and David Laibson, 'Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets' (2006) 121(2) *The Quarterly Journal of Economics* 505; Oren Bar-Gill, 'Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis)Perceptions' (2019) 86 *University of Chicago Law Review* 217; William Allender, Jura Liaukonyte, Sherif Nasser, and Timothy J. Richards, 'Price Fairness and Strategic Obfuscation' (2020) *Marketing Science* <https://doi.org/10.1287/mksc.2020.1244> accessed on 18 October 2023.

70 This type of credit agreements has been the subject of multiple decisions by the Court of Justice; see, recently, Judgment of 18 November 2021, *A. S.A.*, C-212/20, ECLI:EU:C:2020:901. For a legal and economic analysis, see Jarosław Bełdowski and Wiktor Wojciechowski, 'The Poisonous Fruit of Foreign Currency Loans for Consumers in Selected Central European States: The Dilemma for Macroeconomic Policy', in Avishalom Tor and Klaus Mathis (eds), *Consumer Law and Economics* (Springer 2021).

Significant barriers to arbitrage mean it is hard or impossible to transfer the right to receive the performance on the secondary market. An example of a contractual obstacle is a non-transferable ticket. However, it is also sufficient that the costs of organizing this secondary market are so high that it is not profitable to arbitrage. Struggling to enter into contact with consumers who are or would be offered a higher price is the main practical obstacle to arbitrage. In digital environments, both obstacles can be quite significant.

In digital markets, it is quite easy to keep consumers unaware of each other; therefore, there is a real possibility that traders who do not commit to offering only personalized discounts will signal to consumers that they are offering a personalized discount when they do so. The same traders, however, will hardly signal that the personalization practice is disadvantageous to consumers. Under these circumstances, if possible, traders will opt to inform consumers only that the price has been personalized without giving further information. In other words, they will try to hide their exploitative practice behind a curtain of opacity or vagueness.

More precisely, the following outcomes can be identified:

- Outcome 1: the trader commits to offer and offers personalized discounts only
- Outcome 2: the trader may offer personalized discounts or surcharges and offers a personalized discount or the impersonal price
- Outcome 3: the trader may offer personalized discounts or surcharges and, in the end, offers a personalized surcharge

These three scenarios are defined based on traders' pricing strategies: whether they exclusively offer personalized discounts and whether they present consumers with personalized discounts or surcharges. A personalized discount is a tailored price lower than the impersonal price, while a surcharge is higher than the impersonal price. Traders may commit solely to personalized discounts as a strategy to appeal to consumers (Outcome 1). To ensure that consumers are receiving a discount, traders will disclose the impersonal price effectively. This is vital for transparency and maintaining trust. However, if traders do not commit exclusively to discounts, they may give some consumers a surcharge and others a discount (Outcomes 2 and 3).

For strategic reasons, traders might avoid specifying which type of personalized price a consumer is receiving, as revealing a discount to one

consumer might imply a surcharge for another. However, this will happen only if consumers being offered an 'opaque' personalized price can compare it with another consumer's personalized discount. If, instead, consumers even perceive an 'opaque' personalized price as advantageous to them,[71] traders will systematically make their discounts explicit (Outcome 2) and their surcharges opaque or implicit (Outcome 3).

Against this background, the mere right to know that the price is personalized is, quite likely, ineffective in helping consumers. If traders prefer to disclose neither discounts nor surcharges, knowing that the price was personalized may lead consumers to assume optimistically that it is a discount, even when it is not. If traders prefer to disclose discounts for self-interested reasons, consumers may still interpret an 'opaque' personalized price (Outcome 3) as a discount. The result will be clearly dissatisfactory for consumers.

In sum, independently of consumer behaviour, the mere right to know that the price was personalized is not helpful to consumers. This does not mean that an information disclosure should be discarded in general as an important piece of the puzzle necessary that must be solved to make price personalization pro-competitive and pro-consumers.

Exploitative price personalization is quite literally an example of *divide et impera*. The practice aims to identify and exploit consumers who are willing to pay more for the good or service. Thus, the practice specifically targets herd protection, which is characteristic of healthier market contexts.

At the same time, price is a very salient contractual attribute, especially if it is presented in a simple way. This means that even if traders try to separate consumers into smaller groups, if meaningful information is given them in a simple way, the market mechanism could come a long way in deterring exploitative price personalization.

71 There is limited empirical research on this matter. The limited evidence available suggests that consumers interpret opacity optimistically, thereby benefitting exploitative practices. See, Willem van Boom, Jean-Pierre van der Rest, Kees van den Bos, Mark Dechesne, 'Consumers Beware: OnlinePersonalized Pricing in Action! How the Framing of a Mandated Discriminatory Pricing Disclosure Influences Intention to Purchase' (2020) 33 Social Justice Research 331.

II. An information duty that would work?

The core of the information duty I advocate for is the comparison between the personalized price and the personalized one: the right to know of how much the price was personalized. More precisely, traders should disclose the personalized price and the impersonal one at the same time. The simplest way to do so would be to rely on market practices used to make discounts salient. Notably, the information duty would not prohibit personalized surcharges (price increases above the market price) but would force traders to make them salient. The assumption is that the trader would have to justify to the consumer why they should want to pay a higher-than-normal price.

Under EU law, this right to know the impersonal price can also be constructed by way of interpretation of the information duty introduced by the Modernisation Directive. In fact, the text of the directive reads as: "where applicable, [consumers have the right be informed] that the price was personalized on the basis of automated decision-making". Since, as noted above, this mere right to know that the price was personalized is of little (if any) use to consumers, the principles of transparency and effectiveness require more from this text.[72] An attractive norm would grant consumers the right to know how much the price was personalized on the basis of automated decision-making. Important systematic considerations can be extracted by a careful analysis of the General Data Protection Regulation.[73] In particular, a careful analysis of Articles 7 and 22 GDPR supports this view.[74]

Moreover, to consider how intrusive this proposal would be, one needs to consider that is arguably the case that the right to be offered an impersonal price is already granted by the GDPR.[75] In extreme synthesis, in Outcomes 2 and 3, traders try to take advantage of their bargaining power, so that the bundled consent to price personalization and to enter into the contract with the personalized price is plausibly presumed not to be freely given. Accordingly, traders are obliged to give consumers the option to enter into

72 Esposito 2020, n 33, above.
73 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC OJ L 119/1.
74 Esposito 2020, n 33, above.
75 Esposito 2022b, n 34, above.

the contract without consenting to the offering of a personalized price. A similar conclusion can be reached when the legal basis traders try to rely upon is legitimate interest: exploitative price personalization is not a legitimate interest, so consumers can effectively object. This means that the right to be offered the impersonal price exists.

Consequently, recognizing the existence of the right to know how much the price was personalized would simply require making explicit at the relevant moment in time an information consumers are entitled to know anyhow. This does not seem like an enormous interpretative leap, but it is possibly an effective way to protect consumers from many exploitative attempts on digital markets.

G. Conclusions

All consumers can be harmed, not only the 'vulnerable ones' within the meaning of the UCPD. Indeed, all consumers' economic interest, safety and health shall receive a high level of protection pursuant to Article 169 TFEU.

The scenarios of harm are a useful framework to identify the deeper issues behind an intuitively concerning market practice. Thus, the scenarios help assess to what extent and why the practice is problematic, thereby pointing in the direction of plausibly effective interventions.

Throughout the chapter, it was seen that the single most significant variable is to what extent the interests of sophisticated and naïve consumers are aligned. In other words, herd protection is at the core of consumer policy. In terms of legal interventions, this means it is often reasonable to rely on empowerment tools, first and foremost, information duties. Empowering sophisticated consumers in the benchmark and lemon scenarios can go a long way to make traders behave fairly.

At the same time, one needs to see when empowering is unlikely to work. This is especially the case in the scenarios of harm called *divide et impera* and bottom scenarios. in these scenarios, empowerment of sophisticated consumers is unlikely to help naïve consumers. Thus, more intrusive forms of intervention will be needed, to the benefit of all consumers, but especially the naïve ones.

The semi-final point to make is that the theory of harm approach implies that the legal system should react with particular resolution in those situations where traders are or at least have been actively operating to misalign the interest of sophisticated and naïve consumers.

The final point is that the extent to which sophisticated and naïve consumers' theoretical categories overlap with the legal ones of average and vulnerable consumers requires careful investigation. The correlation cannot be simply assumed. Some choice architectures could be so complex that reasonably informed attentive and circumspect consumers are best understood as naïve consumers; this essentially means that the market is best understood as an instance of the bottom scenario, thereby requiring strong legal intervention.

Information, Transparency and Fairness for Consumers in the Digital Environment

Emilia Mišćenić[*]

A. Introduction: consumer legislation in the digital age – fit for purpose?

Technological developments and increasing digitalization have brought multiple challenges to EU consumer law. We are faced with new and digital technologies that are changing the environment in which the average consumer is acting on the market and in everyday transactions. The question is: are these changes for better or worse? At this point, the Commission is questioning digital fairness between businesses and consumers in online transactions and the adequacy of EU consumer law to answer the challenges of digitalization.[1]

At the same time, this chapter addresses critically the position of the consumer in the EU digital market. An average consumer, 'who is reasonably well informed and reasonably observant and circumspect', becomes weak and vulnerable when stepping into the digital market.[2] The reasons for this are manifold, as will be described in the chapter. While some of the reasons causing 'digital vulnerability' can be attributed to the consumer as a person, a variety of reasons for this arise from the digital environment as well as risks related to the developing digital market and digital technologies.[3]

---

* This work has been partially supported by the University of Rijeka projects Transparency and Fairness in the Digital Environment (uniri-iskusni-drustv-23-101) and Efficient regulation of digital market to boost innovation in ICT sector (uniri-drustv-18-214).

1 European Commission, Digital Fairness - Fitness Check on EU consumer law, available at <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en>.

2 Mišćenić, E, 'Legal Risks in Development of EU Consumer Protection Law' in Miscenic and Raccah (eds), *Legal Risks in EU Law: Interdisciplinary Studies on Legal Risk Management and Better Regulation in Europe* (Switzerland: Springer International Publishing, 2016) 135.

3 Helberger, N, Lynskey, O, Micklitz, H-W, Rott, P, Sax, M and Strychar, J, *EU Consumer Protection 2.0, Structural asymmetries in digital consumer markets*, BEUC (2021).

In line with these recent developments, this chapter addresses the position of consumers on the digital market and focuses on the relation among information, transparency, and fairness in the digital environment. This chapter also addresses the gap that exists not only between 'digital fairness and transparency', but also between legal regulation and the digital reality. Despite the existing legal framework, businesses are only purportedly complying with legal rules. More often than not, they are circumventing or ignoring the requirements of EU consumer law related to mandatory information duties and transparency. This has been proven so far by diverse empirical research and studies, as well as CJEU case law on violations by businesses of information duties and transparency. Cases such as *Tiketa*, *Meta Platforms Ireland*, *Victorinox*, *Fuhrmann-2*, and many others,[4] demonstrate how speedy development of digital technologies is affecting businesses-to-consumer (B2C) relationships and contributing to 'digital asymmetry' between businesses and consumers. What cases such as these also point to is the need for change and adjustment of the current legal rules on mandatory information duties and transparency, as will be discussed in the chapter.

In the digital environment, where our choices are not run by rational and informed decisions but manipulated by design and various digital techniques and unfair commercial practices, such as dark patterns and profiling, all of us tend to transform from an average to a vulnerable consumer. Not only do we not know or understand that we have been manipulated by unfair digital techniques, we also do not possess the knowledge and the expertise needed to understand the highly complex mechanisms running the algorithms or the programming language of distributed ledger technologies.[5] Once we step into the digital market, which is shaped by its own features and particularities and bears risks that we are not familiar with, we simply have no other choice but to click and accept in order to get a product or service. As consumers, we are ticking different boxes, accepting cookies, privacy policies, standard terms and conditions (T&C), mostly

4 CJEU, Case C-536/20, 24.02.2022, *Tiketa*, ECLI:EU:C:2022:112; case C-319/20, 22.04.2022, *Meta Platforms Ireland,* ECLI:EU:C:2022:322; case C-179/21, 05.05.2022, *Victorinox* ECLI:EU:C:2022:353; case C-249/21, 07.04.2022, *Fuhrmann-2,* ECLI:EU:C:2022:269.

5 Paterson, M, 'Misleading Al: Regulatory Strategies for Algorithmic Transparency in Technologies Augmenting Consumer Decision- Making' (2023) *Loyola Consumer Law Review* 558 (558 *et seq*). See also Galli, F, *Algorithmic Marketing and EU law on Unfair Commercial Practices* (Springer, 2022) 181.

without reading them or without getting important information prior to concluding a contract on a durable medium.

It is precisely at this point where the reality differs from legal regulation and its requirements. As will be demonstrated, traders' T&C usually incorporate pre-contractual information as required under EU consumer directives or at least some of the required information. According to Commission sweep actions, two out of three web shop sites were not properly informing consumers of their right to withdraw from the contract within 14 days, as well as of other rights in cases of non-conformity, nor were they informing consumers about the possibility of online dispute resolution.[6] Depending upon the web design, traders' T&C are available online via hyperlink and are often changed unilaterally by the trader without a valid reason or without informing the consumer.[7] The consumer is not in a position to negotiate the T&C, and even if they get them, they do not understand them. This undermines substantive transparency requirements as interpreted by CJEU case law, according to which the contract should set out transparently the specific functioning of the agreed arrangement and consumers must be able to evaluate the economic consequences which ensue from it.[8]

The digital techniques and practices described create an environment in which digital fairness is replaced by increasing unfairness caused by non-transparency in online B2C transactions.

B. What is going on in the EU legislative arena?

Currently we are faced with extra-production and over-production of various legal acts affecting the EU digital single market. Speedy development of online marketplaces and digitalization, as well as a significant increase

6 European Commission EU-wide screening ('sweep'), Online shopping: Commission and Consumer Protection authorities urge traders to bring information policy in line with EU law, 31.01.2020, available at <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_156>.

7 Loos, M and Luzak, J, *Update the Unfair Contract Terms directive for digital services*, European Parliament, PE 676.006 –February 2021.

8 On the extensive CJEU case law see Commission Notice, Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts [2019] OJ C323/04.

in online transactions,[9] has resulted in over-extensive adoption of EU legal acts addressing various issues, in particular information duties and transparency requirements. The General Data Protection Regulation (GDPR),[10] the Digital Services Act (DSA),[11] the Digital Markets Act (DMA),[12] the P2B Regulation (EU) 2019/1150,[13] as well as numerous consumer law directives regulating different sectors or particular legal institutions are all relevant for the status and role of actors on the digital market, foremost for their rights and obligations in B2C online transactions.

In an online transaction, B2C relationships can, for instance, be covered by:

- the Consumer Rights Directive (CRD) regulating distance contracts, pre-contractual information duties, and withdrawal periods,[14]
- the Unfair Contract Terms Directive (UCTD) regulating the fairness of the content of contract provisions,[15]

9 Eurostat, E-commerce statistics for individuals, Last update: February 2023, available at <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals>.

10 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 L119/1.

11 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277/1.

12 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265/1.

13 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11 July 2019, 57–79.

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

15 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95.

- the Unfair Commercial Practices Directive (UCPD) addressing a variety of traders' manipulative practices, such as dark patterns or other misleading and aggressive commercial practices,[16]
- the Omnibus Directive improving regulation and protection in online transactions by addressing some more recent developments and actors on the market, such as influencers or sponsored advertising,[17]
- the Twin Directives regulating possible lack of conformity of goods or digital content or digital services,[18]
- the Product Liability Directive regulating producers' liability for defective products,[19]
- the E-Commerce Directive addressing the information duties and responsibilities of information society providers,[20]
- the Electronic Communications Code regulating specific technical requirements related to electronic communications services and networks,[21] as well as the rights and duties of operators and their end-users, including consumers, and

16 Directive 2005/29/EC of the European Parliament and Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ L 149.

17 Directive (EU) 2019/2161 of the European Parliament and of the Council 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, OJ L 328, 18.12.2019.

18 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.5.2019; Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136, 22.5.2019.

19 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210/29.

20 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178/1.

21 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ L 321/ 36.

– the Payment Services Directive 2 regulating customer authentication and faster and more secure electronic payments,[22]
– etc.

In addition, current initiatives and proposals for amendments to some of these legal acts are afoot, either because these are outdated or because they need further improvement and adjustment to the goals of sustainable development.[23]

This development is highly relevant for the topic of transparency and digital fairness and for all actors on the digital market, both businesses and consumers. Businesses in all their forms – sellers, suppliers, operators, online platforms and search engines, payment services providers and many others – all have to comply with different requirements and obligations regulated by all or some of these acts and pay high compliance costs. Even so, they cannot be really sure that compliance has been fulfilled properly and in accordance with all existing EU legal rules.

Consumers and other customers, on the other hand, can barely grasp and understand their rights and obligations arising under all these rules, let alone find them on the interface of a certain web-page. The information duties prescribed by diverse legal acts have lost their real purpose in practice – in particular in the digital environment, which significantly affects transparency requirements.

Moreover, and as expected, these legal acts contain many flaws that often overlap or need further clarification and interpretation of different vague and general legal terms. For instance, it is still unclear when and if certain intermediaries, such as online platforms under the DSA, are included in the definition of 'trader' under the CRD or 'seller' under the

22 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337/35.

23 Eg, Proposal for a Directive of the European Parliament and of the Council on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394, Directives (EU) 2019/771 and (EU) 2020/1828, COM(2023) 155 final; Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final; Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM/2022/496 final; 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.

Twin Directives, or when they are liable.[24] Of course, one can rely on the interpretation in CJEU cases, such as *Kamenova*, *Whatelet*, *Eventim*, *Tiketa*, or European Commission interpretation guidelines.[25] However, businesses and consumers acting on the digital market are usually unaware of CJEU rulings and cannot be expected to wait for dispute resolution or guidelines to get the right answer on how to act on the market.

Another example is the discussion on how to categorize the role of influencers on the market. Many influencers advertise various third-party products and services in exchange for certain benefits and their services are widely used by traders.[26] The legal solution is to be found in several EU legal acts, such as the E-Commerce Directive imposing duties on information society services providers, and the UCPD as amended by the Omnibus Directive. The latter amendments helped in clarifying the role of influencers on the digital market, by requiring that a third party operating on the market and offering products must state if they are a trader or not.[27] Prohibition of fake reviews and introduction of provisions on paid sponsorships will also increase transparency in relation to influencers, who are now obliged to state if a promotion was paid for.[28]

---

24 See Cauffman, C, 'New EU rules on business-to-consumer and platform-to-business relationships' *Maastricht Journal of European and Comparative Law*, XX(X) (2019) (1) 8 and Carvalho, JM, Arga e Lima, F and Farinha,M, Introduction to the Digital Services Act, Content Moderation and Consumer Protection, *Revista De Direito E Tecnologia* 3 (2021) 1 (71) 99. Under Directive (EU) 2019/771, Rec 23: 'Member States should remain free to extend the application of this Directive to platform providers that do not fulfil the requirements for being considered a seller under this Directive'.

25 Legal scholarship is divided about the CJEU interpretations and does not answer clearly whether conclusions from case C-149/15, *Whatelet*, ECLI:EU:C:2016:840 can by analogy be applied to online platforms as traders. In *Tiketa*, the CJEU held 'that intermediary and the principal trader may both be classified as "traders" for the purposes of that provision, without there being any need to establish the existence of a twofold provision of services' (para 54). In *Eventim*, the CJEU confirmed that an online booking platform is covered by the concept of 'trader' within the meaning of Art 2(2) CRD.

26 European Parliament Study, Michaelsen, F, Collini, L, Jacob, C, Goanta, C, et al, *The impact of influencers on advertising and consumer protection in the Single Market* (2022); Riefa, C and Clausen, L, 'Towards fairness in digital influencers' marketing practices' *Journal of European Consumer and Market Law* 8 (2019) 2 (64) 64.

27 Đurović, M, 'Adaptation of Consumer Law to the Digital Age: EU Directive 2019/2161 on Modernisation and Better Enforcement of Consumer Law' (2020) 68(2) *Belgrade Law Review* 62–79.

28 Arts 6 and 7 UCPD. According to the Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning

Another example is dark patterns that are prohibited by Article 25 DSA, but at the same time are not covered and excluded from the UCPD. According to Article 25(2) DSA the prohibition in paragraph 1 on manipulative online interface design affecting a free and informed decision by service recipients will not apply to practices covered by the UCPD or GDPR. There is no clear explanation why a certain unfair commercial practice, in particular one directly affecting B2C relationships, could not be prohibited by both legal acts.

All of this creates a high degree of legal uncertainty for market players, who have to adjust to speedy development of the digital market and who have to know precisely their rights and duties, let alone their position and the role on the market. However, new and upcoming legislation seems to complicate things even further by adding more requirements and offering less by way of guidance and practical solutions. The increase of legal fragmentation is putting legal certainty and transparency at risk.

This is not a novelty *per se*, in particular in EU consumer law, where academics warn that an uncoordinated and unsystematic regulatory approach is of much more harm than use to all the addressees of such excessive legal regulation. Over the years, we have witnessed many attempts to improve the legal framework of EU consumer law in the form of different agendas and initiatives. In the New Consumer Agenda 2020, the Commission questioned whether further and additional legislation is needed to ensure an equal level of consumer protection in online and offline B2C transactions.[29] Two years later, the Commission launched an initiative on 'Digital fairness – Fitness check on EU consumer law' aimed to assess whether existing pieces of legislation are ensuring a high level of protection in the digital environment. The Fitness Check is focused on the legal adequacy of the three main EU consumer directives – namely the UCTD, the UCPD, and the CRD – in terms of the current demands of the digital environment. The questionnaire that forms part of public consultation launched on 28

unfair business-to-consumer commercial practices in the internal market, *OJ C 526/1, 2.2., influencers* 'could qualify as traders if they engage in such practices on a frequent basis, regardless of the size of their audience. Alternatively, in case the persons do not qualify as traders, they could nevertheless be considered to act 'on behalf of' the trader whose products are promoted by the practice and therefore fall within the scope of the Directive.'

29 Communication from the Commission to the European Parliament and the Council New Consumer Agenda – Strengthening consumer resilience for sustainable recovery, COM(2020) 696 final.

November 2022 reveals that the aim of the initiative goes beyond assessing the three directives but also the state of play on the EU digital market since the last check in 2018.[30]

Particular questions deal with vitally important issues, such as the coherence of EU consumer law with other sector-specific laws, for example data protection, new rules applicable to online platforms, artificial intelligence, and so on. EU consumer law refers only partially to application of other areas of law, while these areas insufficiently address consumer protection. For instance, the GDPR refers to the UCTD in its Recital 42 concerning a subject's consent to data processing in preformulated declarations.[31] There seems to be more coherence with the DSA, which is 'without prejudice to Union law on consumer protection' (Recital 10 DSA). However, similarly as with the DMA, certain unfair commercial practices are insufficiently addressed, which in turn opens the door to potentially harmful and unfair commercial practices in the digital environment.

This means that the bond between EU consumer law and other areas of law needs to be strengthened. Other questions tackle vital consumer issues, such as dark patterns and manipulative designs, consent to online contracts, and availability of traders' T&C, conclusions, prolongations and cancellations of digital subscription contracts, as well as the role of influencers on the digital market.

For instance, question no. 1 addresses 'digital practices that unfairly influence consumer decision-making', while question no 2. asks about consent to T&C and making their content easily understandable to a consumer. Questions related to termination and cancellation of digital subscription contracts discuss proposals on informing and reminding consumers. The question about free trial subscription asks about sharing sensitive information about consumer payment details with traders.

The questionnaire also investigates whether the concept of an 'average' or 'vulnerable' consumer needs further benchmarks or criteria in order to adapt to the digital environment. Regardless of the question asked in the Fitness Check public consultations, there is a clear horizontal thread that brings them all together. This relates to information and transparency. This

30 European Commission, A New Deal for Consumers: Commission strengthens EU consumer rights and enforcement available at <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3041>.

31 According to Rec 42 GDPR preamble the pre-formulated declaration of consent '... should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms' in accordance with the UCTD.

chapter therefore aims to clarify the position of consumers in relation to businesses on the digital market and to examine how they are affected by information and transparency requirements.

C. From an average to a vulnerable consumer in the digital environment

Are we all vulnerable in the digital environment and, if so, why? In order to offer a plausible answer, we need to start from the beginning and draw a clear distinction between the basic concepts, namely the definition and the image or concept of the consumer. The definition of the consumer differs from one directive to another, but it usually contains two cumulative criteria defining the consumer as a natural person who is acting on the market outside of their business or professional purposes. For instance, Article 2(2) of Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods (SGD) defines the consumer as 'any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft or profession'.

Many CJEU judgements interpret the notion of consumer in different EU consumer directives and in relation to different circumstances, including both of the two criteria, and related notions, such as dual purpose contracts, for example *Gruber*, *Costea*, *Schrems*, *Di Pinto, Faber*, *Šiba* and many others.[32] However, these will not be discussed within the context of this article. What is to be discussed here is the concept, also known as the image, of the consumer existing behind these definitions that arise under various EU consumer directives. It is precisely the image that is decisive for a better understanding of the position of the consumer as a person acting on the market and their relationship towards businesses, that is, traders.

As noted above, over the years, CJEU case law and several EU consumer directives, have developed different consumer concepts.[33] It is therefore not surprising that the Fitness Check is questioning whether further bench-

32 CJEU Case C-464/01, *Gruber*, ECLI:EU:C:2005:32; case C-110/14, *Costea*, 03.09.2015, ECLI:EU:C:2015:538; case C-311/18, *Facebook Ireland and Schrems*, ECLI:EU:C:2019:1145 case C-361/89, *Di Pinto,* 14.03.1991, ECLI:EU:C:1991:118; case C-497/13, *Faber,* 04.06.2015, ECLI:EU:C:2015:357; case C-537/13, *Šiba*, 15.01. 2015, ECLI:EU:C:2015:14.

33 Leczykiewicz, D and Weatherill, S, *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law* Oxford Legal Studies Research Paper No. 9/2016 (Hart Publishing, Oxford 2016)); Stuyck, J, '*Consumer Concepts in EU Second-*

marks and criteria are needed to draw a clear distinction between the 'average' and the 'vulnerable' consumer.

Both of these concepts are reflected in CJEU case law and referred to in EU consumer legal acts. When interpreting the UCPD provisions in *Gut Springerheide,* the CJEU developed the concept of an average consumer, 'who is reasonably well informed and reasonably observant and circumspect'.[34] This concept evolved over the years and now represents a benchmark for consumer protection in interpretation of various EU consumer directives (the CRD, the UCTD as listed above). So, despite being initially recognised as a concept bound to unfair commercial practices,[35] today it represents a benchmark used in interpretation in cases related to unfair contractual terms, consumer credit, sales contracts, and so on. The role of the average consumer is nevertheless prone to changes and, depending upon the circumstances of the case, the position of a particular consumer can easily transform into a weak consumer, who is 'in a weak position vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge.'[36]

The consumer can also be ignorant and unaware of their rights,[37] or vulnerable for a variety of reasons.[38] For instance, vulnerability is recognised under the UCPD and the CRD because of consumers' 'mental, physical or psychological infirmity, age or credulity'.[39] Unlike a definition itself, the concept of the consumer changes, in particular in situations in which special personal and factual circumstances affect the position and consequently the behaviour of the consumer towards traders.[40] For this

---

ary Law' in Klinck and Riesenhuber (eds), *Verbraucherleitbilder: Interdisziplinäre und europäische Perspektiven* (de Gruyter, 2015) 120.

34 CJEU Case C-210/96 *Gut Springerheide* ECLI:EU:C:1998:369, para 31.

35 Duivenvoorde, BB, *The Consumer Benchmarks in the Unfair Commercial Practices Directive* (Springer 2015) 159.

36 CJEU joined cases C–240/98 to C–244/98, *Océano Grupo and Salvat Editores,* ECLI:EU:C:2000:346, para 25.

37 CJEU Case C-32/12, *Duarte Hueros*, EU:C:2013:637, para 38.

38 CJEU Case C-382/87, *Buet and Others v Ministère public*, 16.05.1989, ECLI:EU:C:1989:198, para 13; case C-149/15, *Wathelet*, 09.11. 2016, ECLI:EU:C:2016:840, para 39. See European Commission, Consumer vulnerability across key markets in the European Union, Final Report, 2016, available at <https://commission.europa.eu/system/files/2018-04/consumers-approved-report_en.pdf>.

39 Rec 34 CRD; Art 5(3) UCPD and Rec 18.

40 Purnhagen, K, 'More Reality in the CJEU's Interpretation of the Average Consumer Benchmark – Also More Behavioural Science in Unfair Commercial Practices?' *European Journal of Risk Regulation* 8 (2017) (437) 439; Purnhagen, K and Schebesta,

reason, behavioural studies play an important role in understanding the concept of a consumer.[41]

What we often witness in practice is a transformation from an average to a weak or rather vulnerable consumer depending upon the circumstances of the case. For this purpose, it would be useful to determine when and under what circumstances an average consumer becomes a vulnerable one, in particular in the digital environment. Does every average consumer become vulnerable when stepping into the digital world or engaging in an online transaction? Both parties to B2C relationships and other market players would certainly benefit from some additional benchmarks and clarification of these questions.

Many different aspects of vulnerabilities are recognized in EU consumer law, such as physical, intellectual, and economic vulnerability. The question is: how do these affect the position of the consumer on the market? Is someone vulnerable prior to stepping into the digital market? Or do they become so because of the risks and demands of the market?

The concept of vulnerability is particularly recognized in the context of financial services, such as consumer and mortgage credit agreements and other services.[42] As emphasised in the Payment Account Directive, EU legislation 'must effectively take into account the needs of more vulnerable consumers'.[43] Here, the consumer often crosses the line of being average and becomes vulnerable, not only because of their financial needs and personal situation, but also because of the high risks associated with the highly complex functioning mechanisms of financial, banking, or payment services and products. In these transactions the consumer becomes more vulnerable and deserves enhanced protection.

This suggests that a clearer distinction is needed between vulnerability in general and so-called 'digital vulnerability'. In general, vulnerability is to be looked at from two main angles, one related to the specific needs

H, 'Island or Ocean: Empirical Evidence on the Average Consumer Concept in the UCPD' (2020) 28 (2) *European Review of Private Law* 293–310.

41 Incardona, R and Poncibò, C, 'The average consumer, the unfair commercial practices directive, and the cognitive revolution' *J Consum Policy* 30 (2007) 21.

42 Reich, N, 'Vulnerable Consumers in EU Law, in Leczykiewicz, D and Weatherill, S, *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law* (n 33) (141).

43 Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic feature, *OJ L 257/214.*

of a person acting on the market, and another related to the specifics of the market and its products. As emphasised by Waddington, vulnerability can be linked to both endogenous (factors inherent to the individual) and exogenous (external) factors.[44] In the context of the digital environment, Recital 34 CRD requires that in providing clear and comprehensible information before the consumer is bound by a distance contract:

> the trader should take into account the specific needs of consumers who are particularly vulnerable because of their mental, physical or psychological infirmity, age or credulity in a way which the trader could reasonably be expected to foresee.

Article 5(3) UCPD applies similar criteria when determining particularly vulnerable specific groups, such as elderly people or children. Article 5 ODR Regulation requires that:

> the ODR platform is accessible and usable by all, including vulnerable users ("design for all"), as far as possible.[45]

The concept of vulnerability is important to online traders and other businesses, who need to take into account the specific needs of consumers when informing them about their rights and obligations and other important aspects of an online transaction.

When it comes to the digital market, we all tend to transform from an average to a vulnerable consumer, because we lack the capacity to understand the complex language of IT technology, algorithms, programming language, and distributed ledgers technologies. The products and services offered on the digital market – and the market itself – are less transparent due to use of the highly complex technological, mathematical and algorithmic mechanisms on which they are based. As rightly pointed at by Weber, the consumer does not understand 'the programming language and the techniques of the distributed ledgers having Java similarities or being Python or

44 Waddington, L, 'Exploring vulnerability in EU Law: An analysis of 'vulnerability' in EU criminal law and consumer protection law' (2020) *45*(6) *European Law Review*, 779–801, 782.

45 Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) OJ L 165, 18.6.2013, 1–12.

Solidity', nor are smart contracts or blockchain technology expressed in an 'understandable language'.[46]

At all stages, from advertising, precontractual informing, contract conclusion as well as in the post-contractual stage, consumers are at risk because of either their personal position or of the specifics of the digital market and its products and services. This makes the structural imbalance of power between businesses and consumers much worse in the digital environment and leads to digital asymmetry, where our choices are not run by rational and informed decisions, but quite often manipulated by algorithms and other digital techniques, such as dark patterns, profiling, manipulative design, and so on.[47]

All in all, one can conclude that in the digital environment there is still a place for all of the above-mentioned concepts, including the average consumer acting in ordinary B2C online transactions. However, due to use of different manipulative designs and unfair digital techniques, as well as the risks inherent to the digital market, vulnerability is more likely to occur in the digital environment. According to the BEUC report from 2021:

> …digital vulnerability describes a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations and the very architecture of digital marketplaces.[48]

Under the New Consumer Agenda 2020:

> the vulnerability of consumers can be driven by social circumstances or because of particular characteristics of individual consumers or groups of consumers, such as their age, gender, health, digital literacy, numeracy or financial situation.

In short, it would be useful to develop additional benchmarks, as has already been done by some Member States, such as Spain, where the legis-

46 Weber, R, 'The Disclosure Dream – Towards a New Transparency Concept in EU Consumer Law' (2023) (12) 2 *Journal of European Consumer and Market Law (EuCML)* (67) 69.

47 Costa, E and Halpern, D, 'The behavioural science of online harm and manipulation, and what to do about it', Discussion paper, Behavioural Insights team (2019).

48 BEUC 2021 (n 3) 5.

lator introduced further criteria to determine the category of vulnerable consumers.[49]

D. Information duties in EU consumer legislation and CJEU case law

I. Information duties

The structural imbalance of power in B2C relationships is worsening in the digital environment, in particular in relation to the bargaining power that consumers are usually left without, the level of knowledge related to AI and digital technologies, and information asymmetry between the parties. In the digital environment, one talks about different aspects of vulnerability, such as digital illiteracy or lack of awareness about digital risks. However, while literacy and awareness are highly recommended and needed, empirical studies confirm that even literate and aware consumers make wrong choices. This usually occurs not because of digital illiteracy, but simply because they are manipulated by unfair digital techniques.

Consumer choices are affected by online behaviour tracking, by use of personal data for business purposes, by manipulative designs, as well as by other sorts of dark patterns.[50] And behind every manipulation lurks misuse of information. Although digital asymmetry cannot be cured by the right to 'right' information, it is most likely that the situation can be improved by greater transparency and more effective regulation of mandatory information obligations.[51]

---

49 Response of the European Law Institute, European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law (2023) 34: 'According to Art. 3.2 of the General Consumer Protection Law… vulnerable consumers with regard to specific consumer relations are those natural persons who, individually or collectively, due to their characteristics, needs or personal, economic, educational or social circumstances, are in a special situation of subordination, defencelessness or lack of protection that prevents them from exercising their rights as consumers under equal conditions, even if this is territorial, sectoral or temporary'. For other measures in non-EU countries see OECD, 'Consumer Vulnerability in the Digital Age' (2023) 355 *OECD Digital Economy Papers* 34.

50 Bongard-Blanchy, K, Rossi, A, Rivas, S, Doublet, S, Koenig, V, Lenzini, G, 'I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous! - Dark Patterns from the End-User Perspective', DIS '21: Designing Interactive Systems Conference 2021, 763–776.

51 Segger-Piening, S, 'No Need to Read: 'Self-Enforcing' Pre-Contractual Consumer Information in European and German Law' in Mathis and Avishalom *Consumer Law*

So, where do we stand today with regard to legal regulation of information duties? In order to answer this question, several aspects need to be addressed, where the first concerns current legal regulation on disclosure and mandatory information obligations, as well as the question how it affects an average or vulnerable consumer.

Despite extensive criticism from legal scholarship and elsewhere, EU consumer law still insists upon provision by businesses of extensive mandatory information to consumers in order to cure information asymmetry and obtain a balance in B2C relationships. This paternalistic approach to legal regulation is the residue of outdated views according to which an average consumer, who is reasonably well informed, as well as reasonably observant and circumspect will be empowered by the information and therefore come to an informed and reasonable choice and decision.[52] For instance, the CRD prescribes more than twenty pieces of information to be provided both at the pre-contractual stage and once the contract has been concluded.[53] More than nineteen pieces of pre-contractual information are to be provided on the Standard European Consumer Credit Information (SECCI) form in consumer credit, together with the option of providing additional information to consumers by creditors.[54] The Mortgage Credit Directive (MCD) requires extensive information to be included in advertising (Article 11), general information (Article 13(1)(a)-(n)), pre-contractual personalized information (Article 14(1)) to be provided in the European Standardised Information Sheet (ESIS), and further information on intermediaries and representatives (Article 15).[55] The forthcoming Consumer Credit Directive (CCD 2) follows this pattern and regulates advertising (Article 8), general information (Article 9), pre-contractual personalized information on the basis of SECCI (Article 10), as well as information for

and Economics, *Economic Analysis of Law in European Legal Scholarship* (Springer 2021) 89–117.

52 Pichonnaz, P, 'Information Duties' in Micklitz and Twigg-Flesner (eds), *The Transformation of Consumer Law and Policy in Europe* (Oxford, Hart 2023) and literature quoted therein.

53 Art 5(a) to (h) and Art 6 (a) to (t) CRD.

54 Directive 2008/48/EC of the European Parliament and Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, OJ L 133/66, Art 5.

55 Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010, OJ L 60/34.

specific types of credit on the basis of ECCI (Article 11). Use of the proposed one-page Standard European Consumer Credit Overview (SECCO) was heavily discussed during the legislative procedure.[56]

The content of mandatory information to be provided by businesses – that is, traders – to consumers is most likely to overlap in certain fields of legal regulation with respect to the digital environment as well. For instance, the E-Commerce Directive sets requirements for information society services providers regarding online information, online advertising, online shopping, and online contracts. It requires provision of clear, comprehensive, and unambiguous minimal information prior to placing an order, and for the T&C to be available in a way that allows storage and reproduction for recipients (Article 10(3)).

The information requirements for different market players, such as online platforms, search engines, and intermediary service providers are regulated by other pieces of legislation, such as the DSA or the P2B Regulation. In addition to the E-Commerce Directive, the CRD and other acts, mandatory information is to be provided to consumers under the ADR/ODR rules,[57] the Twin Directives, and the Omnibus Directive requiring 'additional specific information requirements for contracts concluded on online marketplaces' (Article 6(a)). Particularly interesting and at the same time contradictory is the way in which provision of mandatory information is regulated. EU consumer directives regularly require that an endless sea of information is provided to the consumer by the trader 'in good time before' or 'before the consumer is bound', and in a 'clear and comprehensible manner' (Article 5(1) CRD; Article 6a Omnibus Directive).

So, how can an average consumer, who becomes weak or vulnerable in the digital market, comprehend more than twenty pieces of information about a certain product or service? How can the trader provide the consumer with such an amount of information in a 'clear and comprehensible manner', as required under these and many other EU consumer directives?

56 Proposal for a Directive of the European Parliament and of the Council on consumer credits, COM/2021/347 final.

57 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), OJ L 165/63; Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), OJ L 165.

What we are witnessing here is a direct conflict between regulation of information duties and transparency, where over-extensive and ineffective regulation of mandatory information obligations works to the detriment of both businesses and consumers involved in online transactions.

What we are also witnessing is the gap between current legal regulation and digital market reality. The detrimental effects are not only reflected in the decision-making process and behaviour of consumers, who are rather confused than enlightened by the amount of information.[58] These are echoed in digital and online market practices. There is a huge difference between what is required under EU consumer directives and the digital reality, where the consumer is ticking the 'yes' or 'accept' boxes on use of cookies, privacy policy, personal data, T&C, and so on. Information is usually available online on the trader's web-site and, depending upon the web-design, it is most likely that the legally required pre-contractual information, or at least some of it, will be merged with other contractual conditions in the T&C hyperlink.

In most online transactions, pre-contractual and contractual information – meaning contractual conditions – are not even provided to consumers on a durable medium. As confirmed by different studies, Commission sweeps, and case law, traders and other online businesses, such as online platforms and intermediaries, have found their own way to purportedly comply with legally required mandatory information duties.[59]

II. CJEU case law

Violation of information duties and transparency requirements online is continuously addressed by CJEU case law. Cases arising from different consumer law fields confirm the existing gap between legal regulation and its enforcement in practice. When interpreting the former Distance Selling Directive in *Content Services*, the CJEU took a stand against clicking consent to a hyperlink containing pre-contractual information in the

58 Critically on the information overload and referring to the extensive literature, Pichonnaz (n 52).

59 Mišćenić, E, 'Protection of Consumers on the EU Digital Single Market: Virtual or Real One?' in Viglianisi Ferraro, A, Jagielska M and Selucka, M (eds), *The Influence of the European Legislation on National Legal Systems in the Field of Consumer Protection* (Cedam, 2018) 219–246.

T&C, which were only available online on the trader's website. The CJEU explained that:

> a website such as that in question in the main proceedings, the information on which is accessible to consumers via a link provided by the seller, cannot be regarded as a "durable medium".[60]

The Court further emphasized that:

> …a business practice consisting of making the information referred to in that provision accessible to the consumer only via a hyperlink on a website of the undertaking concerned does not meet the requirements of that provision.[61]

Ten years later, in *Tiketa*, the CJEU came to a different conclusion. The Court acknowledged the development of digital technologies and market and accepted clicking on the T&C hyperlink as a way of informing consumers. It stated that the CRD:

> must be interpreted as not precluding the information referred to in Article 6(1) from being provided to the consumer, prior to the conclusion of the contract, only in the general terms and conditions for the provision of services on the intermediary's website, which that consumer actively accepts by ticking the box provided for that purpose, provided that that information is brought to the consumer's attention in a clear and comprehensible manner.[62]

Nonetheless, the CJEU required that information duties are fulfilled and provided to a consumer on a durable medium and concluded that:

> such a means of providing information cannot act as a substitute for providing the consumer with the confirmation of the contract on a durable medium, within the meaning of Article 8(7) of that directive, since this does not prevent that information from forming an integral part of the distance or off-premises contract.[63]

Besides addressing information duties and transparency requirements in the digital environment and in online B2C transactions, the CJEU con-

60 CJEU case C-49/11, *Content Services,* 05.07.2012, ECLI:EU:C:2012:419, para 50.
61 ibid, para 52.
62 *Tiketa* (n 4), para 54.
63 ibid para 54.

firmed and accepted the transformation of the role of pre-contractual information, which in practice actually became post-contractual information.

In other cases, such as *EIS*, the CJEU was dealing with violation of the CRD provisions on information duties and their relation and meaning towards an 'average consumer'.[64] Departing from the concept of an average consumer, the CJEU concluded that:

> in a situation in which a trader's telephone appears on his or her website in such a way as to suggest, to an average consumer, that is to say a reasonably well-informed and reasonably observant and circumspect consumer, that that trader uses that telephone number for the purposes of his or her contacts with consumers, that telephone number must be considered to be "available" within the meaning of that provision.[65]

In *Fuhrmann-2*, dealing with the so-called payment button and the information required under Article 8(2) CRD in cases of online obligatory payments, the CJEU considered that the transparency of information displayed on the button is to be assessed by the national court by taking into account the expectations and understanding of an average consumer. According to the CJEU:

> the referring court will in particular have to verify whether the term 'booking' is, in the German language, both in everyday language and *in the mind of the average consumer* who is reasonably well informed and reasonably observant and circumspect, necessarily and systematically associated with the creation of an obligation to pay.[66]

Only the words appearing on the ordering button or similar function should be taken into account when determining whether the formulation 'complete booking' or similar words correspond to the words 'order with obligation to pay', within the meaning of the CRD provision.[67]

In *Victorinox*, the CJEU was dealing with an online purchase in which the trader omitted to provide information on the existence and the conditions of a manufacturer's commercial guarantee, contrary to the CRD provision on pre-contractual information in distance contracts (Article 6(1)(m) CRD). Here, the CJEU evaluated the trader's duty to provide this information by relying on the legitimate interest of an average consumer

64 CJEU case C-266/19, *EIS*, 14.05.2020, ECLI:EU:C:2020:384.
65 ibid, para 41.
66 *Fuhrmann-2* (n 4), para 33.
67 ibid, para 35.

in obtaining that information for the purposes of concluding a contract. According to the CJEU:

> the information requirement imposed on the trader by that provision does not arise from the mere fact that that guarantee exists, but only where the consumer has a legitimate interest in obtaining information concerning that guarantee in order to decide whether to enter into a contractual relationship with the trader.[68]

Then the Court went further by determining when this legitimate interest exists, 'inter alia, where the trader makes the manufacturer's commercial guarantee a central or decisive element of its offer'.[69] However, in order to determine if the information is central and decisive, or in other words essential information, the CJEU emphasized that:

> account must be taken of the content and general layout of the offer with regard to the goods concerned, the importance of referring to the manufacturer's commercial guarantee for sales or advertising purposes, the space occupied by that reference in the offer, the likelihood of mistake or confusion which that reference *might trigger in the mind of the average consumer* – who is reasonably well informed and reasonably observant and circumspect with respect to the different rights which he or she may exercise under a guarantee or to the real identity of the guarantor – whether or not there might be explanations relating to other guarantees covering the goods, and any other element capable of establishing an objective need to protect the consumer.[70]

In short, CJEU case law is clearly acknowledging development of the digital environment and takes into account the possible digital risks created by misrepresentation or manipulative design and the manner in which these affect the behaviour and the decision-making process of an average consumer.

68 *Victorinox* (n 4), para 53.
69 ibid, para 53.
70 ibid, para 53.

E. The relation between information and transparency in the digital environment

As rightly emphasized by the CJEU in *Radlinger and Radlingerová*, the

> information, before and at the time of concluding a contract, on the terms of the contract and the consequences of concluding it is of *fundamental importance for a consumer*.[71]

But the information should be provided in a transparent and effective manner in order to achieve the goals of EU consumer directives. Ineffective regulation of information duties results in circumvention of legally required information duties and transparency requirements in practice. In the digital environment, usually there is no provision of relevant information in a 'clear and comprehensible manner' and in 'good time before' the consumer is bound by the contract. Carefully designed websites contain catchy information about products and services, while the essential information related to the content, duration, termination, withdrawal or even the exact price, form part of businesses' T&C hyperlink. Those consumers who do click and read, find it difficult to understand and to identify the information that is essential for contract conclusion. Consequently, the current legal regulation of information duties and transparency requirements presents a sort of *l'art pour l'art* that is being ignored or redesigned by online businesses. Moreover, it is not suitable for the digital age, where information is used in a completely different manner than in the offline environment. As stated by Weber, 'transparency or information disclosure must overcome the given challenges and be designed afresh'.[72]

From the very beginning of EU consumer law, information duties were used in consumer directives as a main tool for achieving transparency.[73] According to Riesenhuber and Möslein, 'transparency plays a central role in the capacity of functioning of the market economy' and is often viewed as a synonym for information duties of all kinds.[74] However, in the context

71 CJEU case C-377/14, *Radlinger and Radlingerová*, 21.04. 2016, ECLI:EU:C:2016:283, para 64.

72 Weber (n 46) 69.

73 Howells, G, 'The Potential and Limits of Consumer Empowerment by Information' (2005) 32 *Journal of Law and Society* 349; Đurović, M, *European Law on Unfair Commercial Practices and Contract Law* (Oxford, Hart Publishing, 2016) 192.

74 Riesenhuber, K and Möslein, F, 'Transparenz' in Basedow, J, Hopt, KJ and Zimmermann, R, (eds), *Handwörterbuch des europäischen Privatrechts* (Tübingen, 2009)

of the digital environment, we should ask what is the quality of information, and is excessive information-giving helping or making consumers even weaker and more vulnerable in the digital market? The current legally-required over-excessive information requirements are working to the detriment of both parties, creating high compliance costs for businesses and not providing real protection to consumers.

However, it is not just about 'quantity' but also about the 'quality' of information. Quality is inter alia concerned with the manner in which information-giving should be done in online B2C transactions, and which can significantly contribute to achieving transparency. As emphasised by AG Ruiz-Jarabo Colomer, 'transparency is concerned with the quality of being clear, obvious and understandable without doubt or ambiguity'.[75] As a more general concept, transparency aims to achieve legal certainty through clarity, precision and understandability.[76] And it is precisely the 'quality', including the 'quantity', of information that is currently being questioned in the Fitness Check related to fairness and transparency in the digital environment.[77]

In the context of EU consumer law, many legal acts call for transparency in one way or another, such as the UCTD, the UCPD, the CCD, the MCD, the PSD2, the CRD, the CSD, the DCD, the Omnibus Directive, and more. A variety of legal acts require provision of plain, intelligible, comprehensible, clear and understandable information to consumers. Some of these legal acts introduce further requirements, such as the duty to clarify and explain essential information to consumers. For instance, Article 16 MCD imposes a duty on creditors and intermediaries to provide adequate explanations of pre-contractual information and of essential characteristics of products, as well as of specific effects which might be detrimental to consumers.[78] The DCD provides an explanation in Recital 59 of its preamble, according to which in cases where 'the trader informed the consumer *in a clear and comprehensible manner* before the conclusion of the contract'

1485. Transparency is an important principle in various areas of law (such as public procurement, subsidies, the right to access information) and it contributes to the rule of law and democracy as determined in Arts 6 and 11 TEU.

75 Opinion of Advocate General *Ruiz-Jarabo Colomer* in case C-110/03, *Belgium v. Commission*, ECLI:EU:C:2004:815, para 44.

76 CJEU case C-417/99, *Commission v. Spain*, 13.09.2001, ECLI:EU:C:2001:445, para 40.

77 Fitness Check (n 1).

78 Mišćenić, E, 'Mortgage Credit Directive (MCD): Are Consumers Finally Getting the Protection They Deserve?' in Slakoper, Z (ed), *Liber Amicorum in Honorem Vilim Gorenc* (Rijeka 2014) 23.

the consumer's digital environment is not compatible with the technical requirements, the burden of proof for lack of conformity should be on the consumer.

Transparency forms part of conditions related to modification of digital content and services in Article 19 DCD, where 'the consumer is informed *in a clear and comprehensible manner* of the modification' (lit. c) and 'the consumer is *informed reasonably in advance*' (lit. d). Article 17(2) in relation to Article 3(5) CSD on commercial guarantees regulates that 'the commercial guarantee statement shall be expressed *in plain, intelligible language*'.[79] Many other examples demand transparency in relation to different regulatory aspects and require provision of clear and comprehensive information to consumers.

However, in order to achieve transparency in B2C online transactions and make information understandable to the average or vulnerable consumer, the information has to be '*available to consumers*' in the first place. Once it has been provided or given by the trader or received by the consumer, one can discuss the clarity and comprehensability of the information. Most of the legal acts mentioned explicitly require availability of information that contributes to transparency. For instance, Article 6 E-Commerce Directive asks for the conditions of promotional offers, competitions and games to be '*easily accessible and be presented clearly and unambiguously*'. It also demands clearly identifiable unsolicited commercial communities 'in order to improve transparency'.[80] Under formal requirements for distance B2C contracts, Article 8 CRD requires availability of information and prescribes that 'the trader shall give the information provided for in Article 6(1) or *make that information available* to the consumer in a way appropriate to the means of distance communication used in plain and intelligible language'. The information is legible, 'in so far as that information is provided on a durable medium' (Article 8 CRD). Article 6.a introduced by the Omnibus Directive requires general information on the main parameters determining ranking to be made available in a specific section of the online interface that is directly and easily accessible from the page where the offers are presented (lit a).[81] Amendments introduced to Annex I UCPD related to sponsored online content and higher ranking

79 De Franceschi, A and Schulze, R (eds), *Harmonizing Digital Contract Law – The Impact of the EU Directives 2019/770 and 2019/771* (CH Beck, Hart, Nomos, 2023).
80 E-Commerce Directive, Rec 30.
81 Art 6a CRD.

of products within the search results require that the provider inform consumers of that fact in a concise, easily accessible, and intelligible form and '*to ensure adequate transparency towards the consumers*'.[82]

Similar requirements regarding transparency arise under legal acts regulating the operations of online traders and intermediaries, such as online platforms and search engines.[83] For instance, Article 5 P2B Regulation requires from online search engines to set out the main parameters determining ranking and provide '*an easily and publicly available description, drafted in plain and intelligible language*'. The recently adopted DSA sets a number of conditions to very large online platforms (17 VLOPs) and search engines (2VLOSEs) that reach at least 45 million monthly active users.[84] These designated companies will have to comply with different sets of requirements contributing to transparency in the digital environment, in particular by monitoring and preventing illegal content and disinformation. However, despite the legal rules according to which information should be made available to consumers in plain and intelligible language and prior to contract conclusion, the digital reality is different, as indeed is seen in CJEU case law. Research studies, such as the 2022 European Commission 'Behavioural study on unfair commercial practices in the digital environment', confirm widespread violation of presented rules and extensive use of unfair commercial practices in the digital environment.[85]

Most common examples of use of unfair digital techniques and manipulative design affecting transparency belong to so-called subscription traps related to free trials and digital subscription contracts that consumers can easily conclude, but not terminate.[86] One could argue that in B2C online

82 Omnibus Directive, Rec 21.

83 Lodder, AR and Carvalho, JM, 'Online Platforms: Towards an Information Tsunami with New Requirements on Moderation, Ranking, and Traceability' 4 (2022) 33 *European Business Law Review*, 537–556.

84 European Commission, Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines, Brussels, 25 April 2023.

85 European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F, Boluda, A, Bogliacino, F, et al, *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report*, Publications Office of the European Union, 2022, available at <https://data.europa.eu/doi/10.2838/859030>.

86 RAND Europe, 'Examining misleading online free trials and subscription traps experienced by European consumers', 2018, available at <https://www.rand.org/randeurope/research/projects/misleading-free-trials.html>; *Forbrukerradet,* 'You Can Log Out, But You Can Never Leave' (2021) available at <https://fil.forbrukerradet.no/wp

transactions the consumer has a right to withdraw from a contract within the prolonged duration period as a sanction for the trader not providing information. As accentuated by Howells, 'the right of withdrawal is best viewed as an extension of the modern policy of protecting consumers by informing them'.[87]

However, the consumer who is unaware of the right to withdraw from a contract within the so-called cooling-off period of 14 days, plus 12 months in the case of omission of information on the right of withdrawal (Articles 9-10 CRD), will most likely not use a right that they were not informed about. Pichonnaz addresses the right of withdrawal as a self-enforcement remedy that has both its benefits and its downsides.[88] As interpreted in *Messner, Heinrich Heine* and other CJEU cases related to online transactions, the right of withdrawal as guaranteed by EU consumer directives 'is to be more than formal'.[89]

Moreover, consumers need protection from omission of other relevant and sometimes essential information. Misleading omissions are covered by the UCPD, according to which:

> *a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information* ... and … this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.[90]

In this respect, the UCPD plays an important role in preserving transparency and protecting consumers from misuse and manipulation of information. As confirmed in *Canal Digital Danmark*, where omission of material information on the total price of the subscription resulted 'in a significant asymmetry of information that is likely to confuse consumers'.[91] Without entering the details of the UCPD, one needs to acknowledge the

---

-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf>.

87 Howells, G, 'The Right of Withdrawal in European Consumer Law, in Schülte-Nolke, H and Schulze, R (eds), *Europäisches Vertragsrecht im Gemeinschaftsrecht*, (Köln 2002) 229.

88 Pichonnaz (n 52).

89 CJEU case C-489/07, *Messner*, 03.09.2009, ECLI:EU:C:2009:502, para 19; CJEU case C-511/08, *Heinrich Heine*, 15.04. 2010., ECLI:EU:C:2010:189, para 54.

90 Art 7(2) UCPD.

91 CJEU case C-611/14, *Canal Digital Danmark*, 26.10.2016, ECLI:EU:C:2016:800, para 41.

role that this important EU consumer directive is playing in guaranteeing the 'quality' of information towards an average or vulnerable consumer acting on the digital market.[92] By defining and prohibiting misleading and aggressive commercial practices, including digital ones, and by specifying these practices in the black list from Annex I as commercial practices which are considered unfair in all circumstances, the UCPD creates a strong bond between information, transparency and fairness in the digital environment.

F. The relation between transparency and fairness in the digital environment

In the digital environment and when entering online B2C transactions, the consumer is usually not provided with pre-contractual information separately from the T&C hyperlink. The pre-contractual and contractual terms are merged in the T&C box that consumers tend to accept without reading. Once the contract is concluded, the consumer receives a confirmation link from which they can download the contractual conditions or even the contract. These practices are in direct conflict with the legal requirements on mandatory information on the basis of which the consumer should be able to decide whether they wish to enter the contract.[93] Once the consumer was provided with the link to the pre-contractual information 'after' contract conclusion, as well as with the contractual conditions, they are usually not able to affect the contract content. Often, they do not understand the T&C that are supposed to be drafted in plain and intelligible language.[94] This is not to mention cases, such as the German *WhatsApp* case,[95] in which the T&C are drafted in English or another language that is not the consumer's mother tongue.[96] Lack of transparency affects consumer choices and leaves them without an actual choice, therefore bringing fairness into question.

92 See the other chapters in this volume.

93 CJEU case C-377/14, *Radlinger and Radlingerová*, 21.04.2016, ECLI:EU:C:2016:283, para 64.

94 European Commission, Luzak, J, Loos, M, Elsen M, et al, *Study on consumers' attitudes towards Terms and Conditions (T&Cs) – Final report*, Publications Office (2020) 4.

95 Urteil des Kammergericht Berlin, case Az. 5 U 156/14, 08.04.2016, available at <http://www.vzbv.de/sites/default/files/whatsapp_kg_berlin_urteil.pdf>.

96 Loos, M, 'Double Dutch: On the role of the transparency requirement with regard to the language in which standard contract terms for B2C-contracts must be drafted' (2017) 2 *Journal of European Consumer and Market Law* (EuCML) 54. Differently, Schmitz, B and Pavillon C, 'Measuring Transparency in Consumer Contracts:

In a digital environment where choices are guided by manipulative designs and other unfair digital practices, where essential information is not available in good time before concluding the contract, and where consumers can enter the contract but not leave – we can hardly talk about transparency and fairness.

The relation between fairness and transparency has been extensively addressed by CJEU case law. For instance, in cases related to the use of unfair commercial practices and unfair terms in different consumer contracts – and in particular in consumer credit agreements – unfairness is often caused by non-transparency.[97] The average or even financially vulnerable consumer is often victim to unfair commercial practices, which according to the CJEU must be taken into account when assessing the unfairness of contractual terms. As stated in *Pohotovosť,* failure to mention essential information may be a decisive factor in assessment by a national court whether a contractual term is transparent and fair.[98] In *Pereničová and Perenič*, related to indication of incorrect and misleading information, the CJEU found that:

> a finding that such a commercial practice is unfair is one element among others on which the competent court may… base its assessment of the unfairness of the contractual terms.[99]

This has been recognized in the Commission Guidance on the implementation and application of the UCPD from 2016 and 2021, according to which '*erroneous information provided in the contract terms is 'misleading*' within the meaning of the UCPD if it causes, or is likely to cause, the average consumer to take a transactional decision that he would not have taken

---

The Usefulness of Readability Formulas Empirically Assessed' (2020) 5 *Journal of European Consumer and Market Law* 191.

97 Golecki M and Tereszkiewicz P (eds), *Protecting Financial Consumers in Europe: Comparative Perspectives and Policy Choices* (Leiden and Boston, 2023); de Elizalde, F, 'Standardisation of Agreement in EU Law. An Adieu to the Contracting Parties?' in Durovic M and Tridimas T (eds), *New Directions in European Private Law* (Oxford, Hart 2021) 29–59. Loos M, 'Transparency Under the UCTD: Could You Please Explain what these Terms are Supposed to Mean?' (2020) 9(1) *Journal of European Consumer and Market Law (EuCML)* 25–27.

98 CJEU case C-76/10, *Pohotovosť,* 21.11.2002, ECLI:EU:C:2010:685, para 82.

99 CJEU case C-453/10, *Pereničová and Perenič,* 15.03. 2012, ECLI:EU:C:2012:144, para 47.

otherwise.'[100] By analogy, these conclusions can be applied to online B2C transactions and online contracts, where the UCPD and the UCTD play an important role in guaranteeing fairness and transparency in the digital environment.[101]

In *Verein für Konsumenteninformation* – dealing with online sales contracts concluded by Amazon EU with consumers resident in other Member States – the CJEU found that the unfairness of a pre-formulated contractual term in the general terms and conditions:

> may result from a formulation that does not comply with *the requirement of being drafted in plain and intelligible language*

under the UCTD.[102] This requirement of the substantive transparency forms part of Articles 4 and 5 UCTD,[103] and is to be interpreted as having the same scope under both provisions.[104]

Settled CJEU case law has drawn a clear distinction between so-called formal and substantive transparency and concluded that the requirement of transparency of contractual terms laid down by the UCTD cannot be reduced 'merely to their being formally and grammatically intelligible'.[105]

---

100 Guidance (n 27); European Commission, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, Brussels, 25.5.2016, SWD (2016)163 final, 21. See Orlando, S, 'The Use of Unfair Contractual Terms as an Unfair Commercial Practice' (2011) 7(1) *European Review of Contract Law* (ERCL) 25.

101 Gardiner, C, *Unfair Contract Terms in the Digital Age, The Challenge of Protecting European Consumers in the Online Marketplace*. (Edward Elgar, Cheltenham, 2022) 9.

102 CJEU case C-191/15, *Verein für Konsumenteninformation,* 28.07.2016, ECLI:EU:C:2016:612, para 68.

103 Under Art 5 UCTD contractual terms offered to consumers in writing 'must always be drafted in plain, intelligible language'. Art 4(2) UCTD regulates exclusion from the unfairness test of terms on the main subject matter of the contract or the adequacy of the price and remuneration, 'in so far as these terms are in plain intelligible language'. See Miscenic, E, 'Uniform Interpretation of Article 4(2) of UCT Directive in the Context of Consumer Credit Agreements: Is it possible?' (2018) 3 *Revue du droit de l'Union européenne* 127, 127–59.

104 CJEU case C-26/13, *Kásler and Káslerné Rábai,* 30.4.2014, ECLI:EU:C:2014:282, para 69.

105 ibid, para 71; CJEU case C-186/16 *Andriciuc and Others* ECLI:EU:C:2017:703, para 59; CJEU case C-609/19 *BNP Paribas Personal Finance* ECLI:EU:C:2021:469, para 42 and many others. See Luzak, J, and Junuzović, M, 'Blurred Lines: Between Formal and Substantive Transparency in Consumer Credit Contracts' (2019) 8 *Journal of European Consumer and Market Law* (EuCML) 97.

According to the interpretations in CJEU case law, the transparency requirement:

> is to be understood as requiring not only that the relevant term should be grammatically intelligible to the consumer, but also that the contract should set out transparently the specific functioning of the mechanism … and the relationship between that mechanism and that provided for by other contractual terms …, so that that consumer is in a position to evaluate, on the basis of clear, intelligible criteria, the economic consequences for him which derive from it.[106]

In most cases the CJEU has applied the standard of the average consumer, but also of the weak consumer[107] by accentuating that the UCTD protection system:

> is based on the idea that the consumer is in a position of weakness vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge

meaning that the requirement:

> that the contractual terms are to be drafted in plain, intelligible language and, accordingly, that they be transparent, must be understood in a broad sense.[108]

Further contributing to transparency is the explanation under Recital 21 UCTD:

> whereas contracts should be drafted in plain, intelligible language, the consumer should actually be given an opportunity to examine all the terms and, if in doubt, the interpretation most favourable to the consumer should prevail.

106 *Kásler and Káslerné Rábai*, (n 103) para 75; *Andriciuc and Others*, (n 104) para 45; *BNP Paribas Personal Finance*, (n 104) para 42; CJEU case C-92/11, *RWE Vertrieb,* ECLI:EU:C:2013:180, para 49; CJEU case C-96/14, *Van Hove* ECLI:EU:C:2015:262, para 51; CJEU case C-348/14, *Bucura,* ECLI:EU:C:2015:447, para 55; CJEU case C-119/17, *Lupean and Lupean* ECLI:EU:C:2018:103, para 32 and many others.

107 Esposito, F and Grochowski, M, 'The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration' (2022) 18 *European Review of Contract Law* 1, 1–31.

108 *BNP Paribas Personal Finance*, (n 104) para 42; *Andriciuc and Others*, (n 104) para 44; *Kásler and Káslerné Rábai,* (n 103) para 39.

The so-called grey list from the UCTD Annex contains a plethora of examples of potentially harmful and unfair contractual terms that we are seeing in so many traders' T&C available online – for instance, the terms:

– 'enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract' (j),

or

– 'enabling the seller or supplier to alter unilaterally without a valid reason any characteristics of the product or service to be provided' (k).[109]

What we are witnessing on a daily basis is switching from unpaid and free trial services to paid services without notification, and changes of the essential elements of the contract such as the price and the content of digital subscription contracts or of a mobile phone subscription contract.[110] The author of this chapter received notification of an increase in the price of mobile phone services, 'because of the overall economic market situation' and without a possibility to terminate the contract. Similarly, like many other consumers, she experienced a unilateral change of the entire subscription contract, that is, replacement with a new one, without any prior or post notification and without her consent to the new contract. What is particularly disturbing about the use of these unfair contractual terms and practices are the providers' explanations, according to which unilateral changes without consumer consent are to be accepted, because this is how it is done in the digital environment.

So, this 'digital consumer', as termed by Mak, is exposed to risks that they are not even aware of, and where the extent of unfair practices is sometimes hard to grasp and deal with in practice.[111] The Fitness Check addresses a variety of issues concerning transparency and fairness – including the well-known problems related to digital subscription contracts – and discusses the idea of introducing reminders before automatic renewal, requiring

109 Loos M and Luzak J (n 7); Commission Notice, Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts [2019] OJ C323/04, 24.

110 Busch C, 'Updating EU Consumer Law for the Digital Subscription Economy' (2022) *Journal of European Consumer and Market Law (EuCML)* 41.

111 Mak, V, 'How can consumer interests be protected when consumer identities are increasingly diffuse?' in Micklitz, H-W and Twigg-Flesner, C (eds), *The Transformation of Consumer Law and Policy in Europe* (Hart, Oxford 2023).

explicit consent for payment data, introducing a termination button, and so on.[112]

While the writing of this chapter was nearing completion, the Commission launched an additional targeted survey complementing the public consultation, which assesses the adequacy of EU consumer protection legislation in the digital environment and its interaction with EU digital legislation, such as the DSA, DMA, GDPR, AI Act, and more.[113] Other valuable projects actually use digital technologies to combat digital unfairness, one such example being CLAUDETTE.[114] This automated detector of potentially unfair clauses in online terms of service aims to help digital consumers to detect unfairness online and improves digital fairness and transparency.[115]

G. Closing remarks and proposals

In line with the current Fitness Check initiative questioning the adequacy of EU consumer protection legislation in the digital environment, it can be stated that many serious and complex issues need to be dealt with. The question is, what can be done about it and how? Currently there are far too many legal acts containing many legal rules which are ignored by businesses and which *de facto* do not protect consumers in the digital environment. Pre-contractual information has lost its initial purpose and has become post-contractual information. The transparency and fairness of this information, together with other contractual terms and conditions, becomes highly questionable once traders purportedly comply with legal requirements in practice.

The combination with different unfair digital practices, such as tracking, profiling, use of manipulative designs and of other dark patterns, under-

112 Response of the European Law Institute (n 47).

113 European Commission, Targeted consultation: Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161, available at: <https://s.chkmkt.com/?e=332289&c=136495868&h=E6E97C3663EC023&l=en>.

114 CLAUDETTE – "automated CLAUse DETectEr" – is an interdisciplinary research project hosted at the Law Department of the European University Institute, led by professors Giovanni Sartor and Hans-W. Micklitz, in cooperation with engineers from the University of Bologna and University of Modena and Reggio Emilia, available at: <http://claudette.eui.eu/about/index.html>.

115 Micklitz, H-W, Palka, P and Panagis, Y, 'The empire strikes back: digital control of unfair terms of online services' (2017) 40(3) *Journal of consumer policy* 367–388.

mines the very aim of the consumer legislation presented in this chapter, that is, protection of average and vulnerable consumers as people. As stated in the 2019 declaration of the Council of Europe:

> fine grained, sub-conscious, and personalized levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions.[116]

In the digital environment, where people's choices and decisions are affected by algorithms and other digital techniques, there is a strong need to redefine and adjust EU consumer protection legislation.

All these issues have been recognized in a great deal of legal writings, research and behavioural studies, as well as by different EU institutional initiatives. So far, there has been a plethora of proposals, which differ depending in terms of their research aims and consumer issues analysed. Many voices are calling for adjusting legal thinking on information disclosure and transparency to the demands of the digital environment.[117] For instance, to these belong proposals on the use of tailor-made and personalized information for individual consumers.[118] If used fairly, as discussed within this chapter, tailor-made information might present the right solution. However, if misused by businesses, personalized law might lead to even more complex issues related to privacy, non-transparency, and unfairness in the digital environment.[119]

In their 2018 research study on transparency and information duties, Seizov, Wulf and Luzak propose a variety of beneficial legal and digital solutions.[120] Among others, the authors suggest improving regulation of

116 Council of Europe, Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes, Decl(13/02/2019)1 as quoted by Koivisto, I, '*The Digital Rear Window*: Epistemologies of Digital Transparency' (2021) 8(1) *Critical Analysis of Law* 78.

117 Mak, V, *Legal Pluralism in European Contract Law* (OUP, 2020) 144–46.

118 Luzak, J, 'Tailor-made Consumer Protection: Personalisation's Impact on the Granularity of Consumer Information' in Corrales Compagnucci, M, Haapio, H, Hagan, M and Doherty, M (eds), *Legal Design: Integrating Business, Design and Legal Thinking with Technology*, Edward Elgar, Cheltenham, 2021, 105–129.

119 Busch, C, 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law', *The University of Chicago Law Review*, 2019, 309–331.

120 Seizov, O, Wulf, JJ and Luzak, J, 'The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU' (2019) 42 (1) *Journal of Consumer Policy*, 149–173.

information obligations by introducing guidelines that would specify how to achieve transparency in online contractual terms.[121] The authors also call for improvement of information design to the benefit of consumers by suggesting possible solutions in the online environment. The authors continued to build upon these proposals in an empirical study and paper on improving transparency and legal certainty in Europe, where they confirmed many of the – here presented – conclusions and offered different proposals.[122]

Similar views are shared by BEUC, which invokes introduction of 'fairness by design' as a horizontal principle.[123] In order to improve transparency towards consumers, Camara Lapuente asserts that the outcome of the information process needs to be optimized and the focus should be put on 'how' information is delivered to consumers.[124] According to Grohowski and others, the decision making process and transparency might be improved by developing algorithmic transparency and explainability, which would make consumers understand the functioning of the algorithmic mechanism and of the various digital techniques.[125]

Like many other scholars, the author of this chapter believes that EU consumer legislation can be improved by optimizing the rules on information duties and transparency.[126] Better regulation of currently over-extensive information duties and of transparency requirements that are, as seen above,[127] formulated in a general and descriptive manner and without practical examples or concretisation, is strongly needed. Instead of overbur-

121 Ibid, 158.

122 Luzak, J., Wulf, A.J., Seizov, O. *et al.*, 'ABC of Online Consumer Disclosure Duties: Improving Transparency and Legal Certainty in Europe' (2023) *Journal of Consumer Policy* 1-27.

123 BEUC framing response paper for the REFIT consultation, Towards European Digital Fairness, 20.02.2023, 5.

124 Cámara Lapuente, S, 'Nuevos perfiles del consentimiento en la contratación digital en la Unión Europea: ¿navegar es contratar (servicios digitales "gratuitos")?' in Gómez Pomar, F and Fernández Chacón, I, (eds), *Estudios de Derecho contractual europeo: nuevos contratos, nuevas reglas* (Cizur Menor, 2022) 331–405, 339.

125 Grochowski, M, Jabłonowska, A, Lagioia, F, and Sartor, G 'Algorithmic transparency and explainability for EU consumer protection: unwrapping the regulatory premises' (2021) 8(1) *Critical Analysis of Law* 43–63.

126 Schaub, M, 'How to Make the Best Mandatory Information Requirements in Consumer Law' (2017) 25(1) *European Review of Private Law* 25; Oehler, A, and Wendt, S, 'Good Consumer Information: the Information Paradigm at its (Dead) End?' (2017) 40 *Journal of Consumer Policy* 179–191.

127 See heading E.

dening the parties to B2C transactions with an endless sea of complex information, better to embrace the 'less is more' approach. Legally, this could be accomplished by amending the current rules and by making them more user-friendly. EU consumer directives could be amended by introducing new and additional provisions which would distinguish between 'essential' and other information. These amendments should draw a clear distinction between essential and all other information to be provided at the pre-contractual and contractual stage, and regulate different formal requirements for both categories.

Provision of essential information to consumers on a durable medium should remain obligatory, while hyperlinking to the rest of pre-contractual information and conditions should be considered in the digital environment.[128] Although the CJEU has argued against hyperlinking in the past (*Content Services*), times and circumstances have changed in the digital environment as acknowledged in *Tiketa*.[129]

In addition, it would be useful to nudge passive consumers to read the essential information and terms displayed in pop-ups or drop-down windows.[130] The amended provisions should require businesses to provide 'essential information' on a durable medium when placing an order (for example, by e-mail), while information to be provided should be limited to the main subject matter and the price, and the parties' main rights and obligations, such as the right to withdraw from or terminate the contract, or access to remedies and legal protection.[131]

The suggested solution could fit in with the Fitness Check proposals on the online disclosure of summarized T&C. Introducing 'an easily understandable summary of the key T&C in an easily accessible manner' could be an acceptable legal solution, under the condition that it contains 'essential information' related to the consumer contract and contractual parties. This information should be transparent so that the consumer, average or vulnerable, really understands the legal and economic consequences arising under that contract. This way, the above-presented CJEU case law on

128 See proposals on the format of information given by Seizov, Wulf and Luzak (n 119) 166.

129 See heading D., II.

130 Scholes, A, Behavioural Economics and the Autonomous Consumer (2012) 14 *Cambridge Yearbook of European Legal Studies,* 297–324.

131 Mišćenić, E 'The Constant Change of EU Consumer Law: The Real Deal or Just an Illusion?' (2022) 70(3) *Belgrade Law Review* 679.

transparency requirements could actually enter the regulatory framework and improve fairness in B2C online transactions.[132]

The proposed adjustments could also contribute to lowering businesses' compliance costs, while balancing between the parties' rights and obligations, as well as the risks involved. Achieving greater transparency could help in better allocation of risks and with liability issues. In this sense, all stakeholders involved could benefit from guidelines which would demonstrate how compliance with the regulatory framework would look in practice.

For instance, the transparency requirements across EU consumer directives could be supplemented by practical examples or guidelines introduced in annexes. These could include practical suggestions on how to disclose information online, by offering examples of how to format information (such as the potential structure and content of the T&C, information about key consumer rights, such as the right of withdrawal). One could argue that similar attempts have been made in certain sector-specific areas, such as consumer credit, where different forms are used to tell consumers of their rights and obligations, as well as potential risks (such as SECCI and, ESIS).[133]

The latter are not comparable with proposals on concretising transparency and information requirements, because these reflect current regulation and overburden the parties with complex information that is not transparent to consumers. Introduction of practical guidelines might prove to be useful to those businesses and consumers who want to comply with the consumer legal framework and who know their rights and obligations, and has the potential to contribute to more responsible behaviour in the digital environment.

This is already happening in the context of enforcement, where EU competent authorities cooperate with some of the main online businesses, such as Google, WhatsApp, Tik Tok and others in order to improve transparency towards consumers and avoid sanctions.[134] To conclude, this chapter pro-

132 See heading F.

133 Similar as the CRD withdrawal form, which is not used in a uniform manner and differs in traders' practices both by its content and visual appearances. See Commission notice Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights 2021/C 525/01.

134 European Commission, Social media and search engines, available at <https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enf

poses regulatory changes to the benefit of all parties involved in online B2C transactions. These changes should aim at adjusting information and transparency requirements to the digital environment. In the digital environment, more transparency can actually be achieved with less information that is 'essential' and transparent to consumers.

orcement-consumer-protection/coordinated-actions/social-media-and-search-engines_en>; European Commission, Consumer protection: Google commits to give consumers clearer and more accurate information to comply with EU rules, available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_367>.

The New Concept of Digital Vulnerability and the European Rules on Unfair Commercial Practices

Mateja Durovic, Eleni Kaprou

A. Introduction

The rising digitalisation of the market has increased the likelihood of some consumers experiencing poor outcomes, particularly those who are vulnerable. A vulnerable consumer can be defined as someone who, due to their personal circumstances, behaviour, personal situation or market in which they act, is especially susceptible to detriment, particularly when the trader is not acting with appropriate levels of care. For instance, a recent Ofcom study demonstrated that an increasing percentage of younger teenagers turn to Google for "true and accurate information," but only a minority can correctly identify camouflaged forms of marketing such as native content and sponsored links. The digital vulnerability itself comes in many forms, it does not limit only to children or elderly population, and understanding of all versions of digital vulnerability is of essential importance and will represent the first step of my research. Moreover, Covid-19 pandemic, besides contributing to a faster pace of market digitalisation eventually resulted in even more vulnerability which remained even now when social distancing is over and has thus also forced the issue of consumer's vulnerability up board agendas.

In the contemporary digital economy, the consumer protection regulatory framework needs, on the one side, to ensure that vulnerable consumers get sufficiently protected, but, on the other side, the regulatory framework must not unreasonably inhibit innovation and further digitalisation of the market. Balance between these values, in reality, is very difficult to secure and this is where the regulatory intervention needs to be particularly cautious.

B. Consumers and the digital age

Technology is moving at a faster pace than ever before and new developments are transforming the marketplace, leading to a global regulatory battle of the digital market.[1] E-commerce is becoming ever more pervasive and many contracts are concluded online. The online environment is becoming the main avenue for receiving information on products and services as well as purchases and complaints handling. Consumer law has to adapt to all these technological challenges and consider whether the existing framework is still able to serve its purpose.

In the race to get ahead we must consider, who is getting left behind? Which are the consumers that are disadvantaged in this environment and what can regulation do for them? This is the question this paper will answer by focusing on consumer vulnerability in the online environment. It will seek to provide a framework for defining and assessing digital vulnerability and make the case that the digital environment is home to a host of challenges that are not well addressed by the current framework for consumer vulnerability in EU law. Furthermore, it will bring forward proposals on how regulators can take digital vulnerability into account within the existing framework and enhance consumer protection.

The chapter adopts an interdisciplinary approach, especially for approaching the topic of digital vulnerability. This is dictated by the interdisciplinary character of the concept of vulnerability, which has been the subject of study from several disciplines. Since the focus of the paper is on the marketplace, empirical and theoretical papers from marketing and especially the sub-area of ethical marketing have been illuminating in gaining a better understanding of digital vulnerability in the context of consumer law. This interdisciplinary analysis is used to inform the legal analysis which is essential for determining the role digital vulnerability is to play in the EU consumer law context.

The scope of the paper is focused on EU consumer law. The paper is going to cover the key instrument of the EU consumer law, the European Directive 2005/29/EC on unfair commercial practices. The European Union is a global leader both in consumer protection, as well as in the digital marketplace, which makes it an ideal foundation for this research. Furthermore, the EU Commission with its publications and surveys is

1 Anu Bradford, Digital Empires: The Global Battle to Regulate Technology (OUP 2023).

showing an increased interest in consumer vulnerability and its impact in transactions.[2]

This is timely research as EU consumer law is going through reform, following the ongoing process of the assessment of the suitability of the existing consumer law rules for the digital age. While an important part of the ongoing assessment process is ensuring that EU consumer law is able to respond to technological challenges, the subject of consumer vulnerability in relation to technology is glossed over. This is what this chapter aims to rectify and place the vulnerable subject in the centre of the discussion. The topic of consumer vulnerability is becoming ever more important in consumer law. This is mirroring broader discussions around the vulnerable subject in law. However, the vulnerable consumer continues to be only secondary to the prevailing image of the average consumer.

C. EU digital environment

To start with, it would be useful to get an overview of the situation in the EU regarding the digital market. This is imperative as the vision for digital vulnerability will depend on the needs that arise from the specific context of the European Union. Already in 2015 the Juncker Commission announced the promotion of the digital single market as a strategic priority for the EU.[3] This is then followed by the Von Den Layen's Commission.[4] The digital single market is viewed as an extension of the single market in the digital world, relevant for all four fundamental freedoms of the Treaties. This choice hardly comes as a surprise as the digital world is becoming ever more important and information technology is becoming more pervasive in all aspects of life. The European Union wishes to establish itself as a

2 See for example, Commission, 'Consumer Vulnerability across key markets in the European Union' (2016) <http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/vulnerable_consumers_approved_27_01_2016_en.pdf> accessed February 2019; European Parliament, 'Compilation of Briefing Papers on Consumer Vulnerability' (2012) <http://www.europarl.europa.eu/RegData/etudes/etudes /join/2012/475082/IPOLIMCO_ET(2012)475082_EN.pdf> accessed October 2023, Pete Lunn and Sean Lyons, 'Behavioural Economics and "Vulnerable Consumers": A Summary of Evidence' (2010).

3 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions:
A Digital Single Market Strategy for Europe, COM(2015) 192 final, 2.

4 The German Presidency of the EU Council, 2020, p. 8.

leader in information technology and reap the benefits of its development, financial or otherwise.

While there is a lot of discussion on the impact of technology, in fact, this is mostly referring to information and communications technologies (ICTs). ICTs in particular, have had a profound effect in many aspects of the economy and broadly of society. They are no longer limited to a specific sector but relevant to all; they are heralded as drivers of development. ICTs are also influential in public affairs, especially when governments use information technologies, usually described by the term e-government.[5] In this setting, consumers have an important role to play. The measures adopted in the context of the Digital Single Market strategy focus on the impact new technologies have on consumer behaviour.[6] The main reference to consumers is in relation to 'better access for consumers and businesses to online goods and services across Europe'. This better access is equated to the removal of trade barriers and differences between online and offline goods. New technologies and their impact on consumers become a vehicle for harmonisation of laws. Arguably, this harmonisation is not only for the benefit of consumers but also for the benefit of traders.

The need of harmonisation of standards is justified by the reported lack of trust of consumers in the digital environment. Consumers appear to have a number of concerns, especially in relation to how their data is being used as well as the security of online transactions. There is something to be said on the emphasis placed on legal environment and consumer rights as the main obstacle for consumers making cross-border online purchases. There is no mention in the strategy of other issues faced by consumers, such as lack of access to hardware or the skills required to navigate the digital marketplace. Furthermore, the image of consumers projected is one of them as passive receivers of the changes brought by new technologies. It ignores the relationship between consumers and the digital market is a lot more dynamic, as consumers are the main drivers of innovation in the sector.

On the one hand, the focus on the cross-border element can be easily explained by the legislative competencies of the EU, as the promotion of the

5 For a review of e-government in the EU, see Lourdes Torres, Vicente Pina, Sonia Royo, 'E-government and the transformation of public administrations in EU countries: Beyond NPM or just a second wave of reforms?', (2005) Online Information Review 29(5) 531-553.

6 COM(2015) 192 final, 5.

internal market is one of the primary objectives of EU consumer law.[7] On the other hand, harmonisation of laws will certainly produce benefits for traders engaging in cross-border trade, while only consumers already taking part in the digital market stand to benefit. It is not clear whether legislative harmonisation could have the effect of attracting more consumers to the digital marketplace.

It appears that the digital skills of consumers and their access to hardware and software are peripheral issues for the EU Commission with the focus being on harmonisation of laws. However, that is not the case when there is no longer talk of consumers, but of workers. There is a social aspect to the Digital Single Market Strategy, with a vision for creating an inclusive e-society citizens and businesses need to have the necessary skills to benefit from technology.[8] Interestingly, there is no talk of consumers as part of this e-society, even though all consumers are simultaneously citizens. Instead, the improvement of digital skills seems to be of paramount importance for another category, that of workers.

The Digital Single Market strategy focuses on the need to develop digital skills for employees so that they can cover the growing demand for ICT sector jobs.[9] There is no mention of improving the digital skills of citizens in order to benefit from the digital marketplace as consumers. Instead, education initiatives focus on the needs of the workplace rather than everyday life or even interaction with public services. Therefore, there seems to be a discrepancy between citizens as consumers who are perceived to possess the necessary skills to participate in the digital marketplace inhibited mostly by security concerns and workers who need to develop their skills to keep up with the needs of an ever-changing marketplace.

Is there a place for digital vulnerability in this fragmented vision of the EU citizen in the digital environment? Yes, indirectly, there is a recognition. A lot of the initiatives center on improving digital skills *and learning across society*. This is an indirect recognition of the existence of digital vulnerability. It shows that the population across EU does not have the same digital skills, as can be expected, and that there is the need to address that. The EU is funding several programmes promoting digital inclusion.[10] However, digital inclusion in this context appears to be a more restricted concept,

7 Art. 26 TFEU.
8 COM(2015) 192 final,16.
9 COM(2015) 192 final,16.
10 For more information on digital inclusion see below.

including primarily disabled consumers.[11] What is telling is that the only programme for social inclusion concerns elderly consumers.

So, while the EU Commission has an understanding of the different needs and skill levels of citizens in the digital environment as well as potential issues with accessibility, there appears to be disconnect between that and their capacity as consumers. Consumers are perceived in this context as passive receivers of the benefits of technology and harmonisation of laws. In order to avoid making assumptions on digital vulnerability, and especially which groups are to be considered disadvantaged in the online environment, one would need to have the relevant empirical data on hardware and internet usage.

Fortunately, there is such a body of data for the EU.[12] While it cannot provide all the answers, it serves to point out general tendencies and is a useful tool to better understand where the EU digital market is now as well as how it evolved over time. For that purpose, there is a special Eurobarometer on E-communications and the digital single market which is published annually since 2006. Prior to that there were frequent Eurobarometer surveys under different names monitoring both the access to hardware e.g. how many households owned telephones and computers as well as the usage of such devices e.g. for internet access, making calls etc. The questions asked, and information collected slightly changes over time, reflecting the technological advances, such as the advent of the smartphone which also provides access to the internet as opposed to personal computers.

The Eurobarometer surveys can provide useful information on how the EU performs as a whole, as well as how the different Member States perform. The main unit of measurement is the household, thus making it less easy to distinguish the demographic characteristics of the population. However, there is also a socio-demographic analysis for certain aspects. Another metric that would be very interesting but is not included is the socio-economic status of respondents. Still, there is a palpable difference between north and south and west and east with the European south and eastern European Member states lagging behind. This suggests that bigger economies tend to perform better and there is greater penetration and

11 For a list of the funded EU projects on digital inclusion please see https://ec.europa.eu/digital-single-market/en/news/eu-funded-projects-digital-inclusion (Accessed November 2023).

12 For all the relevant Eurobarometer data and reports, please see the EU Open Data Portal at http://data.europa.eu/euodp/en/home (Accessed November 2023).

use of new technologies by their citizens. This can serve to point out the importance of income level or socio-economic status in this.

There a re encouraging messages coming out of the latest Special Eurobarometer, such as the fact that internet access is growing in the EU, with a three-point increase since 2015. However, it must be underlined that there are great disparities depending on the country, with Netherlands and Scandinavian countries having 90% access to internet, while southern and Balkan countries are doing the worst.[13] It is the countries with the lowest scores that have done the greatest strides in terms on internet access.[14] This point to geographic location as a factor for digital vulnerability in the EU. For example, a Greek consumer, who might have less access to technology may be more vulnerable compared to a Swedish consumer with almost universal access.

The socio-demographic analysis reveals another key factor for vulnerability, that of age. Elderly consumers appear to have less access to the internet. Elderly consumers are the ones that consistently score poorly in all the relevant categories. The most pronounced differences are in consumers aged over 75. Gender is another factor with women scoring lower than men. Still differences there are not significant. The available data does not suffice to provide a full picture as it cannot provide an answer as to why these differences in relation to age, gender and geographic location occur. Also, it would be helpful to include other factors, such as income, disability or education level to have richer data. It is also important to remember that technology is constantly evolving and this can be observed in the long-term changes in the data, such as the switch to mobile phones rather than computers for internet access.

D. Digital and consumer vulnerability

Vulnerability is a broader concept, used in a variety of disciplines, as well as in different areas of law, focus here is on consumer vulnerability. It is a fuzzy concept that does not have a single definition and often authors that use it do not engage with it sufficiently. [15] In consumer law there is the recognition that consumers are a heterogenous group, encompassing

13 ibid. at 43.
14 ibid. at 45.
15 Kate Brown, '" Vulnerability ": Handle with Care' (2011) 5 Ethics and Social Welfare 313, 315.

people with varied characteristics and abilities. This implies that some will be more vulnerable than others. However, there is a certain disparity between this accepted fact of vulnerable consumers and the legal standard for consumers.

In EU consumer law, there is a renewed interest in consumer vulnerability, both in terms of policy documents, as well as academic publications.[16] Policy documents, such as the recent EU report on consumer vulnerability present a more sophisticated image of consumer vulnerability. One that is influenced by the marketing literature on vulnerability, such as the landmark paper of Baker, Gentry and Rittenburg. [17] Baker, Gentry and Rittenburg with their model have contributed in shifting the attention away from who is vulnerable, to what is vulnerability and viewing it as a state that may be experienced by anyone.[18]

In legal scholarship that trend is less noticeable, with focus still being on defining certain vulnerable groups of consumers. For example, Reich identified the three types of 'consumer vulnerability': (*a*) physical disability, (*b*) intellectual disability, (*c*) economic disability.[19] This tendency can be explained to an extent by the definition of vulnerable consumer in EU consumer law. The key definition for the vulnerable consumer can be found in the Unfair Commercial Practices Directive (hereafter UCPD). While this definition is not employed in other EU directives, it remains highly influential, also due to the broad scope of the UCPD.

Art. 5.3 UCPD states:

> 'Commercial practices which are likely to materially distort the economic behaviour only 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

16 M Friant-Perrot, 'The Vulnerable Consumer in the UCPD and Other Provisions of EU Law' in Willem van Boom, Amandine Garde and Orkun Akseli (eds), *The European Unfair Commercial Practices Directive: Impact, Enforcement Strategies and National Legal Systems* (Ashgate Publishing Group 2014); Norbert Reich, 'Vulnerable Consumers in EU Law' in Dorota Leczykiewicz and Stephen Weatherill (eds), *The Images of the Consumer in EU Law* (Hart Publishing 2016).

17 Stacey Menzel Baker, James W Gentry and Terri L Rittenburg, 'Building Understanding of the Domain of Consumer Vulnerability' (2005) 25 Journal of Macromarketing 128, 128.

18 ibid. at 134.

19 Reich (2016) 141.

trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group'

This is a definition that has been criticised as narrow, as it limits the criteria for vulnerability to that of infirmity, age or credulity. [20] An addition to the UCPD that is confusing and unable to protect vulnerable consumers. [21] Still, this paper is asking something slightly different. Is this definition and the rights provide by EU consumer law able to protect those that are vulnerable in the digital environment? To answer that question, we must consider the factors influencing vulnerability in the online environment and why a special case must be made for digital vulnerability.

E. Related terms

The term 'vulnerability' is not frequently employed for the digital environment; instead the related terms of 'digital divide', 'digital inequality' and 'digital exclusion' are far more common. The use of these terms indicates the outcome of the digital revolution as one that has winners and losers and a sharp distinction between the two. Still, this paper will use the term vulnerability, as one that is in use in consumer law and treats the above terms as explaining vulnerability.

The term digital divide was popularised in the US, in 1999, in the National Telecommunications and Information Administration (NTIA)'s 'Falling Through the Net' report, where the term was defined as the disparities in access to telephones, personal computers (PCs), and the Internet across certain demographic groups.[22] Similar to consumer vulnerability, there is no uniform definition for digital divide. In fact, the origin of the term is disputed. Earlier, digital divide was used not to describe different level of access to technology among users; instead it has been used to describe the

20 JHV Stuyck, E Terryn and TV Dyck, 'Confidence through Fairness?: The New Directive on Unfair Business-to-Consumer Commercial Practices in the Internal Market' (2006) 43 Common Market Law Review 107, 122.

21 R Incardona and C Poncibò, 'The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) 30 Journal of Consumer Policy 21, 29.

22 National Telecommunications and Information Administration (NTIA) (1999) *Falling through the Net: Defining the Digital Divide*. Washington, DC: US Department of Commerce, available at http://www.ntia.doc.gov/ntiahome/fttn99/contents.html. (Accessed November 2023).

opposite camps in relation to technology, those that view technology as positive force that will bring progress and the technophobes that are wary of new technologies and their effects.[23]

The definition of digital divide cannot remain unchanged as it necessarily evolves along with the technology itself. There have already been great strides in the use of technology. For example, a key metric for measuring digital divide or inequality has been access to hardware. That has evolved from access to a telephone to include access to a computer and increasingly, access to a smartphone. Furthermore, there are other aspects that would need to be taken into account today, such as access to internet and internet usage skills. These developments reflect a democratisation of technology and certain technologies becoming more accessible as well as widely used. Personal computers may have been large sized and expensive when first introduced, but they are becoming ever more accessible and easier to use.

This characteristic of new technologies as ever-changing presents challenges that go beyond defining digital vulnerability. Law struggles to keep up with constant changes in technology and their regulation. There is a debate, especially in private law which is our focus, whether the current legal framework can respond to these challenges with some amendments, or whether there is a need for reconsidering the entire legal system in a more radical manner in order to adapt to the changes.[24] The law is not well-suited to being constantly changed and adapted, to the extent that legal certainty is one of its aims.

F. The common elements of consumer vulnerability and digital divide

What has become clear is that the digital divide is not best described as a binary, a sharp distinction between the have and the have-nots, as this approach fails to consider the social resources different groups can contribute.[25] Therefore, it has been argued that the digital divide is best seen as a gradation. This is explained by Warschauer in his example of comparing

23 Dinty W. Moore, The Emperor's Virtual Clothes: The Naked Truth about Internet Culture, (Algonquin Books 1995).

24 Christian Twigg-Flesner, 'Disruptive technology-Disrupted law? How the Digital Revolution Affects (Contract) Law in European Contract Law and the Digital Single Market: The Implications of the Digital Revolution by Alberto de Franceschi (ed), (Intersentia 2016), 21-48, 27.

25 Mark Warschauer, 'Reconceptualising the digital divide', (2002), 7 First Monday 7.

a university professor in the US with a high-speed internet connection to a student in Seoul who occasionally visits an internet café and a rural activist in Indonesia who has no computer or phone line but whose colleagues download and print information for her.[26] In a strict division, all three of these examples would be found to have access to online material, though their circumstances and level of access varies significantly.

This means that the digital divide can be described as relative, meaning that there are varying degrees of intensity experienced by different persons. The same characteristic has been attributed also to consumer vulnerability, meaning there are varying degrees of vulnerability.[27] Vulnerability varies according to the circumstances of the consumer, the market and the transaction. Another key characteristic of consumer vulnerability is its dynamic nature, as vulnerability changes throughout the course of a consumer's life.[28] This is another shared characteristic with digital divide.

In the first years of the development of the internet, around the 1980s-1990s there was a euphoric climate concerning new technologies, such as the internet. There was the view that technology would help humanity overcome the burdens of the past, allow for greater individuality, diversity and above all freedom.[29] However, this has not shown to be the case, and soon after the first enthusiasm came the concern that, in fact, inequality would be exacerbated by technology.[30] While technology is not a cure-all for society's problems, it is clear that it is dynamic and the same can be said for digital vulnerability. Digital vulnerability can vary due to a number of factors, including technology itself, for example, if hardware becomes cheaper and therefore more affordable for consumers who did not have access to them before.

---

26 Mark Warschauer, 'Reconceptualising the digital divide', (2002), 7 First Monday 7.

27 Consumer Affairs Victoria, 'What do we mean by vulnerable and disadvantaged consumers?'(2004),available online at https://www.consumer.vic.gov.au/resources-and-tools/research-studies (accessed November 2023) 4.

28 See for example, Commission, 'Consumer Vulnerability across key markets in the European Union' (2016) <http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/vulnerable_consumers_approved_27_01_2016_en.pdf> accessed November 2023, 44, adopting that position.

29 Esther Dyson, 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2, August 22, 1994)' (1996) The information society 12, no. 3 295-308, 303.

30 Paul DiMaggio, Eszter Hargittai, 'From the 'Digital Divide' to `Digital Inequality':Studying Internet Use As Penetration Increases', (2001). Princeton: Center for Arts and Cultural Policy Studies, Woodrow Wilson School, Princeton University, 4(1), 4-2.

G. Conceptualising digital vulnerability

The conceptualisation of the digital divide has evolved and now reflects a more sophisticated view. An excellent example of that is in the work of Van Dijk on the definition of access.[31] He distinguishes four kinds of barriers to access and the type of access they restrict:

1. *Lack of elementary digital experience* caused by lack of interest, computer anxiety, and unattractiveness of the new technology ("mental access").
2. *No possession of computers and network connections* ("material access").
3. Lack of *digital skills* caused by insufficient user-friendliness and inadequate education or social support ("skills access").
4. Lack of significant *usage opportunities* ("usage access").

This is consistent with what was mentioned above on the relativity of digital vulnerability. It also reflects the particular character of digital technologies where in order to participate a number of factors play a role, such as access to hardware and digital skills. In relation to digital skills, it is important to note that they go beyond operating computers and accessing networks to include also the ability to search, select, process and apply information from many sources.[32] This can have significant implications for consumer law, especially in relation to selecting and processing information. Informational disclosure, even though it has been strongly criticised, it remains one of the main regulatory techniques for consumer law.[33]

Likewise, a unique feature of digital vulnerability is the existence of mental barriers to engaging with technology. There are those that while they have the financial means to have access to hardware and software that would allow them to take part in the relevant market, refuse to do so. Such mental barriers may leave individuals feeling excluded and insecure, yet often they are neglected in the literature on access.[34]

---

31 Van Dijk, Jan. 1999. *The Network Society, Social Aspects of New Media. Thousand Oak*s, CA: Sage

32 Jan van Dijk & Kenneth Hacker, 'The Digital Divide as a Complex and Dynamic Phenomenon', (2003) The Information Society, 19:4, 315-326, 316.

33 Geraint Howells, 'The Potential and Limits of Consumer Empowerment by Information' (2005) 32 Journal of Law and Society 349; O Ben-Shahar and Carl Schneider, *More than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2014).

34 Jan van Dijk & Kenneth Hacker, 'The Digital Divide as a Complex and Dynamic Phenomenon', (2003) The Information Society, 19:4, 315-326, 317.

DiMaggio and Hargitai have also suggested different dimensions to digital inequality, based on the understanding that digital inequality is relative and dynamic.[35]

1) Technical means of how people access the internet
2) Level of autonomy in internet usage
3) Level of skill in internet usage
4) Social support available to the users
5) Purposes for which they use the technology

These dimensions and their importance will fluctuate as time goes on. For example, with the rise in usage of smartphones, autonomy in internet usage is increasing, as opposed to earlier where multiple persons may have shared one computer. For vulnerability, the social support available to users is also of critical importance as it can help users overcome their mental barriers as well as improve digital skills. Based on the analysis above, it is appropriate to make some remarks on digital vulnerability for the purposes of this paper. First, it is worth highlighting the aspects that set the digital marketplace, and by extension digital vulnerability, apart.

1) *Digital technologies as all encompassing.* They no longer signify one sector but impact on and are being employed by all sectors of the economy as well as by public authorities.
2) *High likelihood of detriment for consumers.* As the importance of digital technology is increasing, so is the likelihood of detriment for consumers who may not be able use it accordingly.
3) *Relative and dynamic.* More so than other kinds of vulnerability, for digital vulnerability there is a sense that the situation is improving, this is reflected in particular in the increase of access to hardware and an internet connection in the EU. Still, as mentioned above access is more complex than access to hardware and a connection.

Digital vulnerability may be multi-faceted, yet there are some aspects that will be more relevant to consumer law than others. This is also dictated by the objectives and nature of consumer law. For example, while digital vulnerability may impact on social inequality, there are limits to what

35 Paul DiMaggio, Eszter Hargittai, 'From the 'Digital Divide' to `Digital Inequality':Studying Internet Use As Penetration Increases', (2001). Princeton: Center for Arts and Cultural Policy Studies, Woodrow Wilson School, Princeton University, 4(1), 4-2, 7-8.

consumer law can do to address that. With that in mind, here are some helpful aspects for assessing digital vulnerability

1) Assessing different mediums of communication (e.g is something offered only digitally?_
2) Usability (Assessing design features of hardware, software and webpage design)
3) Presentation of information (this is a key feature in the online environment, to consider not only what kind of information is being conveyed, but also how.)

H. Categories of vulnerable consumers

There can be a number of categories of consumers that can be disadvantaged online, yet due to limited space for discussion, this paper will focus on the categories of vulnerable consumers that are set out in the UCPD, as the key definition for consumer vulnerability in EU law. The criteria for consumer vulnerability presented in the UCPD are those of age, infirmity and credulity. With credulity being a vague problematic criterion that does not allow for a specific group of consumers to be singled out for the purposes of research, this paper will be limited to the criteria of age and infirmity. What about the categories that are left out? E.g. a homeless person or in a precarious living situation who may not have access to the internet- would not fall under any of these categories. Conversely an elderly person with enough money to get the latest iphone but unsure how to use it.

The following piece argues for the need to depart from the definition of the average consumer and for the adoption of the definition of consumer vulnerability proposed by Yap et al.[36] when dealing with digital consumers. This is largely motivated by the fast-paced integration of digital content and dependence on digital services in the life of a consumer. The main issues identified with this fast-paced integration are the lack of time to adapt to the online environment and the online choice architecture, the high action costs, as well as the modified behaviour of consumers when dealing with the online environment.

36 Sheau-Fen Yap, Yingzi Xu, LayPeng Tan, 'Coping with crisis: The paradox of technology and consumer vulnerability' (2021) 45 International Journal of Consumer Studies, 1239.

I. The façade of the average consumer

The average consumer is a legal construct used to determine whether the rights of the consumers are respected and to avoid instances in which businesses take advantage of consumers by imposing unfair terms or by employing unfair commercial practices. The average consumer is an individual who is reasonably well-informed, observant and circumspect.[37] This construct is prevalently employed in determining whether a contract term is fair or unfair. Employing the concept leads to an unrealistic standard for consumers who are often the victims of heuristics and can be manipulated by businesses through behavioural economics. Thus, the legal construct seems to work against the consumer rather than come to their rescue when abused by market-leading businesses.

The issues brought by the average consumer construct are even more concerning in the online environment. The main cause of this is the completely different behaviour of consumers when it comes to reading and agreeing to terms and conditions online. It has been shown that consumers skim rather than read the information presented and are more responsive to recommendations.[38] In addition, Weinreich et al. found that out of the pages surveyed 25% had been displayed for less than 4 seconds, 52% of the visits lasted less than 10 seconds, with only 10% of visits lasting longer than 2 minutes.[39] This highlights the lack of attention paid by consumers when it comes to activating in the online environment.

There are two prevalent issues present in the online environment that should highlight the vulnerability of consumers activating in the online environment. First, the complexity of language and the use of pre-selected options influences consumers as it determines them to agree to less favourable policies. Jachimowicz et al. showed that a default is 27% more likely to be selected out of two options.[40] Thus, by exploiting this modified behaviour, businesses are able to ensure a higher rate of agreement with their potentially unfair terms and conditions.

37 Case C-26/13 *Kásler v OTP Jelzálogbank Zrt* [2014] 2 All ER 443, para 74.

38 Geoffrey Duggan, Stephen Payne, 'Skim reading by satisficing: evidence from eye tracking' (2011) proceedings of the SIGCHI conference on human factors in computing systems, 1141.

39 ibid.

40 Jon Jachimowicz, Shannon Duncan, Elke Weber, Eric Johnson, 'When and why defaults influence decisions: A meta-analysis of default effects' (2019) 3 Behavioural Public Policy, 159.

Second, even if defaults had not been used and the consumers were equipped to understand the information presented, the aforementioned privacy policies still remain too long. McDonald and Cranor have shown that the average time that would be required to read privacy policies adds up to 244 hours per year.[41] Coupled with the shorter attention spans of users, it is undeniable that the cost of becoming familiar with the information is too high for consumers. Hence, consumers often agree to the terms without reading them as they may believe that as a lot of other consumers had priorly accepted the same terms and conditions, these cannot be 'that' harmful. Thus, it is evident that rather than being observant and circumspect these consumers rather operate in an unfamiliar environment.

L. An appeal to recognise the vulnerability of consumers

Another relevant legal construct is the vulnerable consumer. These consumers attract a lower threshold that they must satisfy to show that a commercial practice may be unfair. This construct has been defined in Article 5(3) of the Unfair Commercial Practices Directive[42], 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 of credulity in a way which the trader could reasonably be expected to foresee'. This construct has been brought about to highlight the lack of familiarity with different environments of particularly sensible groups.[43] These groups are often defined by an inability to navigate the marketplace, falling victim to the imbalance of power in the business-to-consumer relationship. The role of the vulnerable consumer concept is to ensure equality of bargaining power while preserving freedom to contract. The exact borders of this concept tend to be unclear especially in the UK due to the need to protect the caveat emptor principle.

41 Aleecia McDonald, Lorrie Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 Journal of Law and Policy for the Information Society 543, 550.

42 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').

43 ibid.

Although the most common age groups that are emphasised in debates surrounding vulnerable consumers are the young and the elderly, it is possible to observe that vulnerability may be created by external factors such as pandemics.[44] This was observed in the context of the COVID-19 pandemic which forced consumers to become dependent on the online environment. Yap et al. define consumer vulnerability as 'a temporary and fluid state of powerlessness stemming from the inability of consumers to cope with the uncertainty and instability brought by sudden unforeseen disasters such as human-made disasters and natural disasters that threaten lives and disrupt the functioning of a community or society. Powerlessness occurs when consumers experience a lack of control or agency in consumption goals, and ultimately leads to a loss of consumer welfare'.[45]

It is submitted that the aforementioned definition of the vulnerable consumer is able to accommodate the vulnerability of consumers acting in the online environment better than the one provided by the Unfair Commercial Practices Directive. The digital vulnerability of consumers is architectural as the digital choice architects create it by abusing behavioural economics.[46] In the digital world, vulnerability concerns the inability of consumers to make uninfluenced decisions and the impossibility of preventing businesses from influencing consumers' desires, behaviour and decision-making process.

In addition, the high action costs involved in the online environment increase the vulnerability of consumers who choose to remain unaware of the terms that they agree to when making use of products and services. In addition, the inclusion of consumers activating in the online environment in the category of vulnerable consumers may incentivise businesses to develop more favourable privacy policies as it would be easier to show that terms are unfair.

44 Sheau-Fen Yap, Yingzi Xu, LayPeng Tan, 'Coping with crisis: The paradox of technology and consumer vulnerability' (2021) 45 International Journal of Consumer Studies, 1239.

45 ibid. at 1241.

46 Natali Helberger, Marijn Sax, Joanna Strycharz, Hans Micklitz 'Choice Architecture in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45 Journal of Consumer Policy 176, 187.

M. Conclusive remarks

In conclusion, it has been shown that consumers activating in the online environment cannot and should not be equated with the average consumer who is observant and circumspect. The low attention spans of online users as well as the high action costs demanded by the online environment argue for the expansion of the 'vulnerable consumer' category and the inclusion of consumers activating in the online environment in this class where the threshold of showing that a contract term or a commercial practice is unfair is lower. In addition, it has been argued that the definition of consumer vulnerability proposed by Yap et al. shall be adopted as it accounts for digital vulnerability.

Digital asymmetry captures the position of imbalance between traders and consumers online, alongside the embedded vulnerability of consumers. Such imbalance and vulnerability are: (1) *relational* (due to the position they have in a complex digital environment where equal interaction is made impossible), (2) *architectural* (due to the way user interfaces are designed and operated), and (3) *knowledge-based* (as the trader benefits from detailed insights about the consumer while the consumer often knows - or understands - very little about how the trader and the service operate).[47]

Because digital asymmetry automatically embeds all digital consumers with innate vulnerability, "vulnerability as an exception to the average consumer benchmark becomes less useful to assess the behavioural distortion an interface could cause".[48] Thus, it was vital that the European Commission has acknowledged that the UCPD average consumer benchmark must be interpreted in light of these changing market realities, so as to accommodate vulnerabilities or any other seemingly exceptional circumstances that may actually be cultivated by interfaces themselves.[49] Regrettably, this approach "falls short in addressing the scale of the problem".[50] A more holistic and extensive reform of the UCPD will be required to thoroughly adapt consumer law regulations to the fluctuating digital economy.

47 ibid.

48 https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf.

49 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.

50 https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf.

The Metaverse and Consumers' Vulnerabilities

Niti Chatterjee, Gianclaudio Malgieri[*]

A. Introduction

In the age of relentless technological advancement, the virtual and augmented realms are rapidly melding with our physical world. The emergence of the 'Metaverse'—an expansive digital universe blending augmented reality (AR) and virtual reality (VR) technologies—ushers in an era of immersive experiences that challenge the very fabric of our understanding of presence, interaction, and digital boundaries. Yet, as this expansive digital universe unravels, the implications for its end users, especially the vulnerable ones, grow more pronounced and intricate.[1]

This chapter embarks on a comprehensive exploration of the intertwined realms of the Metaverse and its influence on end users in a situation of vulnerability.[2] Beginning with a dive into the definitional aspects of AR and VR, it strives to demystify the immersive technologies that constitute the backbone of the Metaverse. It sheds light on the intricate sensors and the burgeoning domain of emotion recognition in AR/VR devices, which promise to make digital interactions more intuitive but also present new challenges.

A significant facet of this exploration pertains to wearable devices. These wearables, as intimate extensions of our physical selves in the digital realm, have the potential to induce new types of vulnerabilities in end users. They could also exacerbate existing areas of concern, transforming minor vulnerabilities into major threats. These wearables, while enhancing immersion

---

* Niti Chatterjee contributed mostly to Part I and II. Gianclaudio Malgieri contributed mostly to the Introduction and Part III.

1 Carlotta Rigotti and Gianclaudio Malgieri, 'Human Vulnerability in the Metaverse' (2023) Alliance for Digital Human Rights (AUDRI) Report Series <https://audri.org/resources/report-human-vulnerability-in-the-metaverse/>.

2 Gianclaudio Malgieri, *Vulnerability and Data Protection Law* (Oxford University Press 2023).

and user experience, necessitate a deeper probe into their broader implications.

Vulnerability, a term often laden with complex socio-legal connotations, is re-evaluated in the context of digital consumption and, more specifically, within the realm of AR/VR technologies. How does the Metaverse amplify existing vulnerabilities? In what ways might it induce new ones? These critical questions are dissected, laying the groundwork for a broader contemplation of the overarching impacts on end-users.

By venturing into these complex discussions, this chapter aims to foster a nuanced understanding of the Metaverse's vast potential and the attendant ethical, legal, and societal challenges it poses, especially for those at the crossroads of vulnerability.

I. Demystifying immersive technologies

1. Definitional Aspects

In order to understand how the metaverse and associated immersive technologies may impact end-users of these technologies, it is important to highlight the definitions and key identifiers of AR/VR technologies.

a) AR Technology

AR adds digital elements to the natural/physical world by *"overlaying computer-generated information on reality*" irrespective of place or object.[3] Such placement of digital details (objects/animations) enhances the users' real-world[4] and enables decision-making through added information that users cannot detect using their 'human' senses.[5] Typically, AR projects computer-generated elements on display screens like smart glasses (*e.g.*, Google

3 Donna Berryman, 'Augmented Reality: A Review' (2012) 31 Medical Reference Services Quarterly 212.

4 Bernard Marr, 'The Fascinating History And Evolution Of Extended Reality (XR) – Covering AR, VR And MR' (*Forbes*, 17 May 2021) <https://www.forbes.com/sites/bernardmarr/2021/05/17/the-fascinating-history-and-evolution-of-extended-reality-xr--covering-ar-vr-and-mr/> accessed 8 January 2023.

5 Ronald Azuma, 'A Survey of Augmented Reality' (1997) 6 Presence: Teleoperators and Virtual Environments 355.

Glass), mobile phones, or dedicated headsets.[6] It 'expands' the physical world by relying on a digital 3D depiction of our surroundings ('*digital twin*') to link physical environment to the digital object.[7] A combination of access controls to hardware, alongside specialized software and AI, powers AR technology. Since physical reality is an essential component of AR,[8] access to a camera-equipped device is required to recreate a digitalized version of the physical environment.

Popular examples of AR include games like Pokémon Go[9] or Instagram/Snapchat filters.[10] In the consumer market, AR-enabled interactive products have demonstrated a 94% higher conversion rate for shoppers.[11]

b) VR Technology

Unlike AR, physical environment is not requisite for VR. It comprises technologies that *"simulate interactive virtual environments … with which users become subjectively involved and … feel physically present*".[12] VR completely 'virtualizes' the user's physical environment, creates a synthetically fabricated interface,[13] and relies on the user's sensory system ('perception') to emulate their presence in such digital reality. Key elements like immersion, interactivity, and telepresence are used to design "*embodied*" virtual

6 Lucia Jasenovcova, 'What Is Augmented Reality and How Does AR Work?' (*Resco.net*, 10 August 2022) <https://www.resco.net/blog/what-is-augmented-reality-and-how-does-ar-work/> accessed 11 January 2023.

7 Michael Porter and James Heppelmann, 'How Does Augmented Reality Work?' [2017] *Harvard Business Review*.

8 Berryman (n 3) 213.

9 Ji-Young An and Claudio Nigg, 'The Promise of an Augmented Reality Game—Pokémon GO' (2017) 5 Annals of Translational Medicine S11.

10 'Snapchat Lens vs. Instagram Filter: AR as a Marketing Tool' <https://mazingxr.com/en/snapchat-instagram-ar-filter/> accessed 11 January 2023.

11 'What Role Does Augmented Reality Play in Shaping Consumer Behaviour' (*Marketing Mag*, 17 May 2021) <https://www.marketingmag.com.au/tech-data/what-role-does-augmented-reality-play-in-shaping-consumer-behaviour/> accessed 11 January 2023.

12 Isabell Wohlgenannt, Alexander Simons and Stefan Stieglitz, 'Virtual Reality' (2020) 62 Business & Information Systems Engineering 455.

13 ibid 456.

environments where users connect to computers that become invisible to them.[14]

Immersion is "*the degree of reality experienced by the sensory and perceptual system*" in virtual environments *"using interactive devices*".[15] VR surrounds users so that they perceive their presence in a digital world,[16] distinct from their physical reality[17]: a critical aspect for the discussions in this chapter. VR experiences are often so realistic and immersive (like real-life experiences) that they have the potential "*to enact profound and lasting changes in us*".[18]

Carefully integrated software and hardware components, including haptic touch, enable a stimulated 'feeling of presence' in VR. Specialized devices are critical to fully experience VR, such as a headset that works as a head-mounted display (HMD) or a computer console to stream content and engage users.[19]

Due to *immersion* and *telepresence* in a controlled environment, VR is extensively used to treat mental health disorders.[20] It has revolutionized user experience and enhanced engagement in the gaming industry.[21] Its impact

14 Kenneth Walsh and Suzanne Pawlowski, 'Virtual Reality: A Technology in Need of IS Research' (2002) 8 Communications of the Association for Information Systems 297.

15 Yongming Pan, 'VR Reality of the Relationship between Augmented Reality and Virtual Reality in the Context of Virtual Reality' (2021) 2066 Journal of Physics: Conference Series 012056.

16 Donghee Shin, 'How Does Immersion Work in Augmented Reality Games? A User-Centric View of Immersion and Engagement' (2019) 22 Information Communication and Society 1212.

17 Mana Farshid and others, 'Go Boldly!: Explore Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) for Business' (2018) 61 Business Horizons 657.

18 Jeremy Bailenson, *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do* (W W Norton & Company 2018) 21.

19 Zaynah Bhanji, 'A New Reality: How VR Actually Works' (*Predict*, 12 October 2018) <https://medium.com/predict/a-new-reality-how-vr-actually-works-663210bdff72> accessed 11 January 2023.

20 Lucia Valmaggia and others, 'Virtual Reality in the Psychological Treatment for Mental Health Problems: An Systematic Review of Recent Evidence' (2016) 236 Psychiatry Research 189; Carlos Coelho and others, 'The Use of Virtual Reality in Acrophobia Research and Treatment' (2009) 23 Journal of Anxiety Disorders 563.

21 Jyoti Gupta, 'How Virtual Reality Is Transforming the Gaming Industry' (20 May 2019) <https://yourstory.com/mystory/how-virtual-reality-is-transforming-the-gaming-ind> accessed 11 January 2023.

on consumer choices is also on the rise, with nearly 30% of surveyed users buying products because of testing them through VR.[22]

2. Sensors in AR/VR Technology

In this chapter, '*AR/VR devices*' or '*wearable devices*' refer to hardware components like smart glasses, dedicated headsets (like HMD), computer consoles, and other controllers (including haptic suits and gloves) that facilitate immersive user experiences, excluding mobile phones.

Notably, there is ambiguity in characterizing the concepts of AR, VR, and MR across institutions, academia, and even businesses,[23] particularly regarding standardized terminology. Recently, the European Parliament (EP) defined the '*metaverse*' as a "*digital simulation of a multidimensional space*" comprising mirrored reality (AR), simulating an entirely new space (VR), or mixing both.[24] Clarifying these terminologies would inadvertently expand this chapter. However, technologies that amalgamate AR and VR are referred to as XR or immersive technologies for our purposes.

As we noted previously, AR and VR combine various elements; for the sake of brevity of this chapter, it is sufficient to recognize that there are overlaps in sensory information processed by both technologies. Below is a high-level understanding of the functional elements in AR/VR devices that influence user experiences, providing context for their impact on human vulnerabilities discussed in Part II of this Chapter.

22 'June 2022 Global Consumer Insights Pulse Survey' (PWC 2022) <https://www.pwc.com/gx/en/consumer-markets/consumers-respond-to-waves-of-disruption/gcis-report-june-2022.pdf> accessed 1 November 2023.

23 Philipp A Rauschnabel and others, 'What Is XR? Towards a Framework for Augmented and Virtual Reality' (2022) 133 Computers in Human Behavior 107289.

24 Mariusz Maciejewski, 'Metaverse' (JURI Committee, European Parliament 2023) PE 751.222.

Table 1: Sensors in AR/VR Devices

Sense	Sensors	AR	VR	Effect	How It Impacts
Sight	Camera(s) (and illuminators) or even infrared sensors in HMD.	✓	✓	Eye tracking by measuring eye activity, pupil positions and gaze movement.[25]	Enables '*foveated rendering*' (to display high-quality graphics by identifying the area where the gaze is located) and '*focus rendering*' (ability to display information about the object that holds the user's gaze and hide other objects/make them semi-transparent).[26] These are useful for **gaze mapping** (providing engagement heatmaps) and understanding behavioral attributes like **near-accurate perception about a person's attention**.[27] Some AR/VR devices undertake 'head tracking' and may undertake 'predictive full body tracking' based on sensor data available through HMD and controllers[28] This enables **increased empathy and deeper connections** in virtual environments.[29]
Touch	Handheld controllers/ haptic gloves and suits.	✓	✓	Gesture/ motion tracking through tactile rendering / force feedback and manipulating de-	Increases 'immersion' experience, creating an overall positive experience and **eliciting higher virtual embodiment for users**.[31] Certain 'full body haptic suits' display the capacity to emulate sen-

25 Josef Erl, 'Virtual Reality: Everything You Need to Know about VR' (*MIXED Reality News*, 16 July 2022) <https://mixed-news.com/en/virtual-reality-guide/> accessed 11 January 2023.

26 Ben Dickson, 'How Eye Tracking Will Enhance the AR and VR Experience' (*TechTalks*, 11 June 2018) <https://bdtechtalks.com/2018/06/11/ar-vr-eye-tracking-foveated-rendering/> accessed 4 February 2023.

27 'Eye Tracking — a Catalyst for Innovation in AR, VR, and MR' (*Tobii*, 2022) <https://www.tobii.com/products/integration/xr-headsets/> accessed 3 February 2023.

28 Matthias Bastian, 'Meta Shows Stunning Full Body Tracking Only via Quest Headset' (*MIXED Reality News*, 23 September 2022) <https://mixed-news.com/en/meta-shows-stunning-full-body-tracking-only-via-quest-headset/> accessed 4 February 2023.

29 '5 Benefits of AR Body Tracking' (*AR Insider*, 30 December 2021) <https://arinsider.co/2021/12/30/5-benefits-of-ar-body-tracking/> accessed 4 February 2023.

Sense	Sensors	AR	VR	Effect	How It Impacts
				gree-of-freedom (**DoF**).[30]	sations of being electrocuted or even standing in the rain.[32]
Sound	Spatial (3D) audio sensors and microphones installed in wearable devices (like HMD).	✓	✓	Mimicking sounds heard in real-life, to create sounds with precise realism[33] and voice command integration.	These allow for **more 'intuitive'** and natural experiences for users, adding **more realistic elements** to the virtual environment.[34]

Additionally, AR/VR devices (like HMD and haptic suits) rely on other sensors like gyroscopes (measure the position of the device), proximity and depth sensors (examine distances/spatial orientation), accelerometers (detect changes in movements) and GPS (detect real-time location) to collect information about the user's natural surroundings.[35]

Thus, AR/VR devices collect and process varied data points, including the user's area of interest, engagement levels, and information about their physical environment. While most data collection is consensual or contractually agreed upon, whether such consent is effectual or impinges on human autonomy remains an open question.

30 Dangxiao Wang and others, 'Haptic Display for Virtual Reality: Progress and Challenges' (2019) 1 Virtual Reality & Intelligent Hardware 136.

31 Grégoire Richard and others, 'Studying the Role of Haptic Feedback on Virtual Embodiment in a Drawing Task' (2021) 1 Frontiers in Virtual Reality.

32 Victor Tangermann, 'VR Company Shows Off Full-Body Suit That Electrocutes You Everywhere' (*Futurism*, 2022) <https://futurism.com/the-byte/vr-company-full-body-suit> accessed 11 January 2023.

33 Gergana Mileva, 'Enhancing Immersive Experiences With Spatial Audio' (9 September 2022) <https://arpost.co/2022/09/09/enhancing-immersive-experiences-spatial-audio/> accessed 4 February 2023.

34 Adobe, 'How AR, VR, and Voice Are Redefining Digital Experiences' (*Adobe Blog*, 2017) <https://blog.adobe.com/en/publish/2017/11/16/ar-vr-voice-redefining-digital-experiences> accessed 4 February 2023.

35 Rebekah Carter, 'How Do Augmented Reality and Smart Glasses Work?' (12 September 2022) <https://www.xrtoday.com/augmented-reality/how-do-augmented-reality-and-smart-glasses-work/> accessed 11 January 2023; Jasenovcova (n 6).

3. Emotion Recognition in AR/VR Devices

The AR/VR experience is augmented through 'avatars' designed as users' alter-egos that can shop online, play games, and socialize across different platforms. Additionally, 'non-player characters' (NPC), developed through AI, act as digital agents[36] and react to the user's emotions/actions within virtual environments.[37]

Emotion is the human reaction to a particular stimulus, generated through changes in brain activity, facial expression, gestures, etc. Eye and gesture tracking are often integrated into AR/VR experiences (see discussions in Para I.1 above). Eye tracking forms a key indicator of emotion,[38] and increases in pupil size indicate "*emotionally toned or interesting visual stimuli*".[39] Eye data can identify various aspects, like health status (*e.g.*, watery eyes), ethnic origin, personality traits, sleepiness/fatigue levels, cognitive processes, preferences, aversions, mental workload, etc.[40]

Eye tracking is an essential parameter of facial emotion recognition (FER), facilitating an understanding of our subconscious mind.[41] This section discusses the utilization of FER in AR/VR (and not the functioning of FER technologies *per se*), although FER technology involves feature ex-

36 'Project CAIRaoke: Building the assistants of the future with breakthroughs in conversational AI' (2022) <https://ai.facebook.com/blog/project-cairaoke/> accessed 11 January 2023.

37 'What Will Chatbots and AI Look like in the Metaverse?' (*Muan Group*, 11 January 2022) <https://www.muangroup.com/what-will-chatbots-and-ai-look-like-in-the-metaverse/> accessed 11 January 2023.

38 Paweł Tarnowski and others, 'Eye-Tracking Analysis for Emotion Recognition' (2020) 2020 Computational Intelligence and Neuroscience.

39 Eckhard Hess and James Polt, 'Pupil Size as Related to Interest Value of Visual Stimuli' (1960) 132 American Association for the Advancement of Science 349.

40 Jacob Leon Kröger, Otto Hans-Martin Lutz and Florian Müller, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking' in Michael Friedewald and others (eds), *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG International Summer School, Switzerland, August 2019, Revised Selected Papers* (Springer International Publishing 2020).

41 JZ Lim, James Mountstephens and Jason Teo, 'Emotion Recognition Using Eye-Tracking: Taxonomy, Review and Current Challenges' (2020) 20 Sensors 2384.

traction and emotion classification,[42] and researchers often employ AR/VR devices to undertake these functions.[43]

Based on a survey of the specifications of AR/VR devices' available in the market, it becomes clear that FER indicators are primarily utilized in enterprise settings as on date. However, with leading companies (like Apple,[44] Meta,[45] and HTC[46]) incorporating eye-tracking capabilities in consumer wearable devices, the technology appears poised for mainstream adoption. The industry views ***eye tracking as the next frontier for the metaverses***,[47] enabling avatars to recreate users' emotions and engage in non-verbal communication.

Other than eye-tracking, emotion recognition systems (*i.e.*, ERS) also use gesture movement[48] and voice recognition. Patent searches reveal that companies like Sony,[49] Microsoft,[50] Linden Research (creators of the game 'Second Life'),[51] etc. hold patents for avatars reacting to users' emotions through gesture tracking and/or voice cues. Given this, AR/VR devices already possess or will soon demonstrate capabilities to track our emotions through myriad mechanisms. Involuntary gestures and other verbal/non-verbal communication methods offer insights into consumers' thoughts,

42 J Anil and L Padma Suresh, 'Literature Survey on Face and Face Expression Recognition', *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)* (2016).

43 Dhwani Mehta, Mohammad Faridul Haque Siddiqui and Ahmad Y Javaid, 'Facial Emotion Recognition: A Survey and Real-World User Experiences in Mixed Reality' (2018) 18 Sensors 416.

44 'Apple Vision Pro' (*Apple*, 2023) <https://www.apple.com/apple-vision-pro/> accessed 13 June 2023.

45 'Supplemental Meta Platforms Technologies Privacy Policy' (*Meta*, July 2023) <https://www.meta.com/nl/en/legal/privacy-policy-updated/> accessed 16 June 2023.

46 'HP Reverb G2 Omnicept Edition' <https://www.hp.com/us-en/vr/reverb-g2-vr-headset-omnicept-edition.html> accessed 4 February 2023.

47 Scott Stein, 'Watching Me, Watching You: How Eye Tracking Is Coming to VR and Beyond' (*CNET*, 21 February 2022) <https://www.cnet.com/tech/computing/watching-me-watching-you-how-eye-tracking-is-coming-to-vr-and-beyond/> accessed 5 February 2023.

48 Gavin Buckingham, 'Hand Tracking for Immersive Virtual Reality: Opportunities and Challenges' (2021) 2 Frontiers in Virtual Reality.

49 Ozlem Kalinli-Akbacak, 'Multi-Modal Sensor Based Emotion Recognition and Emotional Interface', (Patent No. US9031293B2).

50 Charlene Mary Atlas and others, 'Digital Personal Expression via Wearable Device', (Patent No. WO2020013962A3).

51 Jeremiah Arthur Grant, 'Virtual Reality Presentation of Body Postures of Avatars', (Patent No. US10438393B2).

and the availability of such data can enable more intuitive and nuanced 'persuasion' profiles.

Thus, to sum up, AR technology places digital objects/information within physical environment. VR technology immerses the user in the virtual environment. Despite technical differences, both technologies employ a combination of sensors through wearable devices that manipulate sensations of touch, sound, and FoV/ fidelity of sight based on eye-tracking. Additionally, wearable devices may embed ERS that use eye movement, gestures, and voice cues, to identify and detect user reactions. These can be used to potentially gain deeper insights into the user's conscious and subconscious mind, thereby creating avenues for manipulation and inducement/exacerbation of vulnerabilities.

II.Human Vulnerability in the Context of AR/VR

1. Conceptualizing Vulnerability

Etymologically, 'vulnerability' means "*susceptibility to being wounded*"[52] and includes a lack of resilience against possible harm.[53] Vulnerability is multidimensional and multidisciplinary: the notion of 'susceptibility' implies that it draws on the **potential** for harm over its actual occurrence.[54] Generally, vulnerability is contrasted against the "*hyper-autonomous, non-vulnerable man*",[55] an ideal yet fictional character. Autonomy is seen as vulnerability's valued antithesis or opposing force[56] – thus, while autonomy

52 Maria Patrao Neves, 'Article 8 - Respect for Human Vulnerability and Personal Integrity' in Henk AMJ ten Have and Michèle Jean (eds), *The UNESCO Universal Declaration on Bioethics and Human Rights: Background, Principles and Application* (UNESCO 2009).

53 Jonathan Herring, *Vulnerable Adults and the Law* (1st edn, Oxford University Press 2016) 139.

54 Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable Data Subjects' (2020) 37 Computer Law & Security Review 105415.

55 Herring (n 53) 9.

56 Alison Diduck, 'Autonomy and Vulnerability in Family Law: The Missing Link' in J Herring and J Wallbank (eds), *Vulnerabilities, Care and Family Law* (Routledge 2013) 104.

begets *"self-sufficiency and independence*", human vulnerability requires an implicit submission of autonomy.[57]

A "*mature, moderately well-educated, clear thinking, literate, self-supporting person*" is often used as the baseline to measure 'vulnerability', assuming that everyone is alike.[58] Such standardization qualifies certain demographic groups as automatically vulnerable, like children (due to their cognitive development), minorities (due to social marginalization), etc.[59]

Legal frameworks, including the EU's Charter of Fundamental Rights[60] in Articles 21, 24, 25, and 26, use similar standardization to provide special protections for minorities, children, the elderly, and persons with disabilities. However, scholars argue that the concept of a 'vulnerable legal subject' should consider an individual's lifespan, reflecting the various developmental and social stages they pass through.[61] Human vulnerability must consider the social relationships and institutions an individual depends on throughout life.[62] This highlights a fundamental paradox: **vulnerability is both particular and universal**.[63] The universality principle acknowledges that anyone can be susceptible to physical, economic, institutional, or social harm.[64] Yet critics argue that safeguarding potential vulnerabilities risks obscuring actual injuries suffered, thus potentially undermining inequalities in society and institutions put in place to address them.[65] Additionally, it disregards the influence of privilege in shaping social practices.[66] Univer-

57 Martha Fineman, 'The Vulnerable Subject and the Responsive State' (2010) 60 Emory Law Journal 251.

58 Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 International Journal of Feminist Approaches to Bioethics 121, 123.

59 'Categories of Vulnerability – Specific Vulnerable Populations | Yale Assessment Module Training' <https://assessment-module.yale.edu/human-subjects-protection/categories-vulnerability-specific-vulnerable-populations> accessed 16 March 2023.

60 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

61 Martha Fineman, 'Feminism, Masculinities, and Multiple Identities' (2013) 13 Nevada Law Journal 619.

62 Martha Fineman, 'Vulnerability and Inevitable Inequality' (2017) 4 Oslo Law Review 133.

63 Lourdes Peroni and Alexandra Timmer, 'Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law' (2013) 11 International Journal of Constitutional Law 1056, 1058.

64 Ibid.

65 Alyson Cole, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique' (2016) 17 Critical Horizons 260.

66 Frank Cooper, 'Always Already Suspect: Revising Vulnerability Theory' (2015) 93 North Carolina Law Review 1339.

salizing everyone as deserving of special protections could also dilute the concept by itself.

As a midway, bioethical research posits a 'layered approach' to vulnerability, advocating for a dynamic and relational understanding to ensure a flexible application.[67] For instance, using the example of women, Luna notes that vulnerability is based on factors like poverty, illiteracy, and societal attitude to reproductive rights. Simply being a woman may not make someone as vulnerable as being a poor, illiterate woman in a country with limited reproductive rights. This relational aspect of layered vulnerability contextualizes specific personal situations.[68] As Malgieri and Niklas summarize, "*all individuals are vulnerable … but some individuals have more layers of vulnerability,*" and legal protections must be proportional to the "*quantity and quality of layers*".[69]

In essence, "*everyone is vulnerable*",[70] and the state is duty-bound to protect and be responsive to their expectations.[71] Accordingly, vulnerability entrenches the principles of equality and equity.

2. Vulnerability vis-à-vis Digital Consumption

Vulnerability holds conceptual significance in consumer protection. Globally, safeguarding vulnerable consumers remains a priority.[72] EU consumer law also identifies 'vulnerable' groups based on shared characteristics. With the advent of digitalization, society has been profoundly impacted, particularly in consumers' interactions with online marketplaces and the economic value of users' data as the asset fueling innovative business models.[73]

Online consumer vulnerability results extend beyond traditionally identified characteristics in the data-for-services economy. It includes *personal and demographic traits*, *behavioral drivers*, *situational drivers,* and *infor-*

67 Luna (n 58) 133.
68 Florencia Luna, 'Identifying and Evaluating Layers of Vulnerability – a Way Forward' (2019) 19 Developing World Bioethics 86.
69 Malgieri and Niklas (n 54) [2].
70 Herring (n 53) 7.
71 Fineman, 'The Vulnerable Subject and the Responsive State' (n 57) 40.
72 'United Nations Guidelines for Consumer Protection' (UNCTAD 2016) UNCTAD/DITC/CPLP/MISC/2016/1.
73 Elena Agibalova and others, 'Consumer Protection in the Digital Environment' in S Cindori and others (eds), *SHS Web of Conferences* (2021).

mation asymmetry, leading to a power imbalance (where sellers have disproportionately more information about consumers without their awareness).[74] Further, subjective traits of end-users, like *lack of technical understanding* (*e.g.,* the use of IoT and AI technologies in processing data) and *markets/information complexity,* lead to heuristics/rules of thumb.[75] These expanded parameters emphasize the need for a broader and more dynamic understanding of digitally induced end-user vulnerabilities, encompassing concerns like inequality, power imbalance, manipulation, and discrimination.

3. Vulnerability Through the Lens of AR/VR Technology

Recent trends indicate a significant rise in AR/VR adoption amongst consumers, with 75% finding immersive experiences 'valuable and impactful' for retail shopping.[76] However, this popularity could lead to vulnerability exploitation in end-users. This section examines how AR/VR devices may amplify existing concerns or introduce new vulnerabilities.

a) Amplification of Existing Vulnerabilities

Literature indicates that AR/VR devices can exacerbate existing vulnerabilities caused by digital technologies.[77] The topic of Metaverse vulnerability has been addressed by Rigotti and Malgieri in a recent report,[78] where the authors recognize the potential benefits of the metaverse, including empowerment and enhancement of human experiences, especially for those vulnerable offline, but they raise concerns about the exacerbation of social

74 European Commission, Consumers, Health, Agriculture and Food Executive Agency, 'Consumer Vulnerability Across Key Markets in the European Union: Final Report' (Publications Office of the European Union 2016).

75 'Challenges to Consumer Policy in the Digital Age', *Background Report* (OECD 2019).

76 Capgemini Research Institute, 'Total Immersion: How Immersive Experiences and the Metaverse Benefit Customer Experience and Operations' (2022) <https://www.capgemini.com/insights/research-library/immersive-experiences/> accessed 18 March 2023.

77 Juan Londoño, 'User Safety in AR/VR: Protecting Adults' (Information Technology & Innovation Foundation 2023) 7.

78 Rigotti and Malgieri (n 1).

inequalities, digital divide issues, and potential reinforcement of conformity within this virtual realm.

Two key issues vis-à-vis general digital technologies are analyzed to demonstrate how AR/VR could intensify these problems for end-users.

(i) *Choice Architecture & Dark Patterns*:
Default settings in digital architecture hold unquestionable power, as they represent the "*pre-selected option*" recommended by software developers,[79] shaping our online conduct.[80] Users retain defaults due to '*bounded rationality*', undertaking a limited evaluation of alternatives in any situation.[81] In such evaluation, our brains rely on a "*variety of unreliable shortcuts and heuristics*" (cognitive biases).[82] This has led to the emergence of 'dark patterns'[83] or deceptive digital designs that manipulate users to act (mostly) against their interests by leveraging psychological elements.[84] These are widely prevalent in online shopping experiences.[85] Scholars have proposed various taxonomies for dark patterns, classifying them into broad categories comprising *information asymmetry* (like fake countdown timers, trick questions, or hidden costs) and *free choice repression* ('sneak into basket' (where uninvited products are directly placed in shopping carts), or 'roach motel' (where unsubscribing from services is unduly complex)).[86]

79 Jay Kesan and Rajiv Shah, 'Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics' (2006) 82 Notre Dame Law Review 583.
80 Ryan Calo, 'Code, Nudge, or Notice?' (2014) 99 Iowa Law Review 773.
81 Mark Leiser, 'The Problem with "Dots": Questioning the Role of Rationality in the Online Environment' (2016) 30 International Review of Law, Computers & Technology 191.
82 Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Online Manipulation: Hidden Influences in a Digital World' (2019) 4 Georgetown Law Technology Review 1, 21.
83 Harry Brignull, 'Deceptive Patterns - User Interfaces Crafted to Trick You' (2010) <https://www.deceptive.design/> accessed 19 March 2023.
84 Colin M Gray and others, 'The Dark (Patterns) Side of UX Design', *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM 2018).
85 Arunesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1.
86 Mark Leiser and Wen-Ting Yang, 'Illuminating Manipulative Design: From "Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive' (SocArXiv, 12 November 2022) <https://osf.io/preprints/socarxiv/7dwuq/> accessed 20 March 2023.

Tricky wordings in online interactions can confuse even regular users due to inattentiveness or language proficiency, regardless of age.[87] Unsurprisingly, existing dark patterns from traditional user interfaces (UX) can be modified for XR, *e.g.*, requiring users to visit physical stores to unsubscribe from VR retailer's newsletters, increasing the chances of additional purchases.[88] Moreover, embedded sensors in AR/VR devices could give rise to novel 'XR-specific' dark patterns.[89] For instance, haptic feedback from AR/VR devices can be used to design such dark patterns.[90] Haptic grabbing (stimuli through hand-controllers) could deflect users' attention away from specific virtual areas (*e.g.*, constantly providing haptic feedback to someone reading the terms of use or placing objects in their FoV to create obstructions),[91] subtly altering their thought process. Clubbed with gaze mapping of the user's attention (see discussion above in Para I.2), it could significantly change our online behavior through subtle 'nudges'.[92] Thus, tweaks in the UX architecture could facilitate manipulative practices in AR/VR to benefit business interests while users retain the 'illusion of choice'. Virtual objects' realism, immersion, and interactivity will likely compound existing problems, enabling creation of more immersive dark patterns that "*differ significantly from the classic dark patterns*" with more "***profound implications*** *for consumer decision-making*" in virtual environment.[93]

87 Ben Bate, 'How Dark UX Patterns Target The Most Vulnerable' (*Web Designer Depot*, 2018) <https://www.webdesignerdepot.com/2018/01/how-dark-ux-patterns-target-the-most-vulnerable/> accessed 13 June 2023.

88 Xian Wang and others, 'The Dark Side of Augmented Reality: Exploring Manipulative Designs in AR' [2023] International Journal of Human-Computer Interaction.

89 'REPHRAIN White Paper: The Metaverse and Web 3.0' (REPHRAIN National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online 2023) <https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2023/03/Call-for-Papers-by-the-All-Party-Parliamentary-Group-REPHRAIN-Response.pdf> accessed 20 March 2023.

90 Wang and others (n 88).

91 ibid 9.

92 Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (Penguin 2009) 6.

93 Francisco Lupiáñez-Villanueva and others, 'Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation : Final Report' (Directorate-General for Justice and Consumers (European Commission) 2022).

(ii) *Digital Advertisements & Marketing*:
Digital advertisements use sophisticated contextual, behavioral, or segmented targeting, using data analytics of our preferences to increase click-through rates.[94] Data collected from various sources (*e.g.*, data *given* and data *given off*) are utilized in personalized ads and marketing communications to create strategic content *"to optimize the fit with personal characteristics, interests, preferences, communication styles, and behaviors*".[95] Despite privacy concerns and AI 'black-box' criticism, such techniques enjoy both affirmation and negative reception amongst consumers (the *personalization paradox*).[96] Such practices can manipulate consumers by combining personalized practices with adaptable, dynamic technologies that use non-transparent measures to exploit vulnerabilities.[97]
Consumer exploitation studies indicate that data analytics easily assimilate information about users' biases, insecurities, fears, and emotions, with targeting strategies potentially (ab)using internal or external parameters (*e.g.*, financial condition) to influence behavior.[98] Examples include Uber's surge-pricing algorithm linked to low-battery levels[99] and Facebook's ability to target teenagers with depres-

94 Niklas Fourberg and others, 'Online Advertising: The Impact of Targeted Advertising on Advertisers, Market Access and Consumer Choice' (Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament 2021).

95 Nadine Bol and others, 'Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts' (2018) 23 Journal of Computer-Mediated Communication 370.

96 Joanna Strycharz and others, 'Protective Behavior against Personalized Ads: Motivation to Turn Personalization Off' (2019) 13 Cyberpsychology: Journal of Psychosocial Research on Cyberspace.

97 Gianclaudio Malgieri, 'In/Acceptable Marketing and Consumers' Privacy Expectations: Four Tests from EU Data Protection Law' (2021) 40 Journal of Consumer Marketing 209.

98 Nadine Bol and others, 'Vulnerability in a Tracked Society: Combining Tracking and Survey Data to Understand Who Gets Targeted with What Content' (2020) 22 New Media & Society 1996; Joanna Strycharz and Bram Duivenvoorde, 'The Exploitation of Vulnerability through Personalised Marketing Communication: Are Consumers Protected?' (2021) 10 Internet Policy Review.

99 Amit Chowdhry, 'Uber: Users Are More Likely To Pay Surge Pricing If Their Phone Battery Is Low' *Forbes* (March 2016) <https://www.forbes.com/sites/amitchowdhry/2016/05/25/uber-low-battery/> accessed 20 March 2023.

sive traits.[100] Psychological characteristics are easily inferred through digital footprints, and personalization relying on such factors leads to higher levels of persuasion.[101] Geospatial movement (identified through keyboard speed) to detect impairment (*e.g.*, tiredness) coupled with other existing data sets, such as education, personality, or recent life events, are also used in targeting.[102] This creates digital inequality through vulnerability exploitation and reinforces stereotypes by targeting content curated for specific demographic subgroups or characteristics, restricting knowledge access for other groups/individuals (*e.g.*, automobile ads targeted towards only men).[103] Additionally, dark patterns in advertisements and gaming can lead consumers to "*mindlessly click*" highlighted buttons "*in a flow state*".[104]

Virtual stores[105] and XR-enabled advertisements are increasingly commonplace. Studies show that consumers are identifiable with 95% accuracy in AR/VR through < 5 minutes of body motion data.[106] Thus, such technology can gain deeper insights into our behavior, with enhanced personalization through ads extremely likely. AR/VR advertisements include 360° views, projection of digital objects in physical environment as preview (*e.g.*, visualize new furniture in the room), product placements within virtual environment, and *magic mirroring* (enabling users to see themselves in virtual environment).[107] Location-based AR advertisement is also prevalent, such as in Pokémon Go, where users were directed to sponsored physical

100 Sam Levin, 'Facebook Told Advertisers It Can Identify Teens Feeling "insecure" and "Worthless"' *The Guardian* (1 May 2017) <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens> accessed 20 March 2023.

101 Strycharz and Duivenvoorde (n 98) 5.

102 Lauren Willis, 'Deception by Design' (2020) 34 Harvard Journal of Law & Technology 115.

103 Bol and others (n 98) 2008.

104 Willis (n 102) 143.

105 Byoungho Jin and others, 'Consumer Store Experience through Virtual Reality: Its Effect on Emotional States and Perceived Store Attractiveness' (2021) 8 Fashion and Textiles 19.

106 Mark Miller and others, 'Personal Identifiability of User Tracking Data during Observation of 360-Degree VR Video' (2020) 10 Scientific Reports 17404.

107 XR Advertising Alliance, 'The XR Digital Advertising Guide' (2018) <https://advertising.report//Resources/Whitepapers/03abd32e-d1fb-488d-8569-a2cc333c13d3_XRAA_Guidebook_V.1.0.0.pdf> accessed 20 March 2023.

locations through in-game activity to drive commercial interests.[108] In this context, a scenario-construction study[109] identified manipulative advertising techniques in XR, including:

a) misleading experience marketing (*e.g.*, colors of a digital object are synthetically enhanced to look comparably better in virtual environment),
b) targeting consumers during moments of vulnerability (*e.g.*, devices embedded with sensors can detect tiredness),
c) emotional manipulation through hyper-personalization techniques (*e.g.*, advertisement targeting a single user through 'deepfakes'), and
d) distorting reality (by changing the customer's FoV (see discussions in Para I.2)).

Immersive and interactive AR/VR experiences may inhibit a customer's cognitive ability to evaluate advertisements by reducing their resistance powers, making the ad more convincing and manipulative.[110] AR/VR devices with embedded sensors can classify personality traits based on user behavior in virtual stores with over 70% accuracy, providing valuable user insights.[111] In this regard, Heller posits the concept of 'biometric psychography' to identify the practice of utilizing biometrics and psychography to identify a person's interest, theorizing that XR technology "*uses behavioral and anatomical information (e.g., pupil dilation) to measure a person's reaction to stimuli over time*" revealing their "***physical, mental, and emotional state, and the stimuli that caused***" such state.[112]

108 Larry Kim, '9 Need-to-Know Facts on How Pokemon Go Players Engage with Businesses' *INC* (19 August 2016) <https://www.inc.com/larry-kim/9-need-to-know-facts-on-how-pokemon-go-players-engage-with-businesses.html> accessed 20 March 2023.

109 Abraham Mhaidli and Florian Schaub, 'Identifying Manipulative Advertising Techniques in XR Through Scenario Construction', *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021).

110 Dan Grigorovici and Corina Constantin, 'Experiencing Interactive Advertising beyond Rich Media' (2004) 5 Journal of Interactive Advertising 22.

111 Jaikishan Khatri and others, 'Recognizing Personality Traits Using Consumer Behavior Patterns in a Virtual Retail Store' (2022) 13 Frontiers in Psychology.

112 Brittan Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law' (2021) 23 Vanderbilt Journal of Entertainment and Technology Law 1.

Given the quantum of sensory information collected by AR/VR devices over a period of time, including eye data and emotions, this entails a lucrative opportunity for platforms to leverage previously unknown information regarding consumer's mental states and characteristics, to build more nuanced 'persuasion profiles' and employ '*microtargeting*' through advanced neuromarketing. Thus, in XR advertisements and marketing, human vulnerabilities could be exploited in subverted ways that are harder to detect since XR experiences are highly personalized (*hyper-personalization*).

b) Inducement of New Vulnerabilities

Aside from exacerbating existing vulnerabilities, research shows that immersive technologies can be used in ways that can induce new types of vulnerability. While this field is relatively nascent, two specific methods are discussed below.

(i) *Memory Falsification:*
The malleability of the human brain is well-known, and our brain is cognitively trained to rely on past experiences during decision-making.[113] VR technology has successfully treated psychological conditions by coaching patients in "*appropriate responses*" based on the disorder.[114] Alarmingly, children exposed to a 3D-based VR rendition of themselves swimming with whales demonstrated false memory of such experiences sometime later.[115] Research involving adults confirms that our brain is "*more prone to confusing*" VR with reality, furthering evidence that VR stimuli are processed by humans "*in a more naturalistic manner*" with a **higher degree of acceptance** compared to traditional technologies.[116] Combining haptic-touch feedback from

113 Joshua Tremel, Daniella Ortiz and Julie A Fiez, 'Manipulating Memory Efficacy Affects the Behavioral and Neural Profiles of Deterministic Learning and Decision-Making' (2018) 114 Neuropsychologia 214.

114 D Freeman and others, 'Virtual Reality in the Assessment, Understanding, and Treatment of Mental Health Disorders' (2017) 47 Psychological Medicine 2393.

115 Kathryn Segovia and Jeremy Bailenson, 'Virtually True: Children's Acquisition of False Memories in Virtual Reality' (2009) 12 Media Psychology 371.

116 Marius Rubo, Nadine Messerli and Simone Munsch, 'The Human Source Memory System Struggles to Distinguish Virtual Reality and Reality' (2021) 4 Computers in Human Behavior Reports 100111.

products with associative visual cues can increase consumer engagement, positively affecting psychological product ownership and product valuation,[117] ultimately influencing purchase decisions. Thus, memories embedded through VR experiences can be manipulated to bias consumer choices (*e.g.*, by inducing artificial feelings in consumers resulting in biased product associations[118]), which promotes commercial interest and result in a loss of autonomy and freedom in decision-making for consumers.

(ii) *Cross-Reality Concerns*:

Our digital avatars in virtual environment can alter our behavior and self-perception (the *Proteus effect*), for instance, users with taller avatars displayed increased confidence in negotiations.[119] Therefore, embodiment in avatars can impact consumers' psychology,[120] and avatar-related design elements made available by platforms could affect our self-esteem (akin to the effect of AR face-filters[121]) and consequent decision-making. Further, emotional attachment to artificial agents (*i.e.*, NPC) previously limited to VR gaming,[122] could take new meaning in a wider XR-consumer context. With NPCs demonstrating the capability to display sophisticated emotions, it could create positive associations and empathy attachment,[123] increasing the possibility for manipulation. The immersive UX of AR/VR experiences is more adaptable than traditional technologies, enabling a more profound influence on users' behavior and preferences.[124] Such expe-

117 Andrea Webb Luangrath and others, 'Observing Product Touch: The Vicarious Haptic Effect in Digital Marketing and Virtual Reality' (2022) 59 Journal of Marketing Research 306.

118 Mhaidli and Schaub (n 109).

119 Nick Yee and Jeremy Bailenson, 'The Proteus Effect: The Effect of Transformed Self-Representation on Behavior' (2007) 33 Human Communication Research 271.

120 Olivia Petit and others, 'Consumer Consciousness in Multisensory Extended Reality' (2022) 13 Frontiers in Psychology.

121 Ana Javornik and others, 'Augmented Self - The Effects of Virtual Face Augmentation on Consumers' Self-Concept' (2021) 130 Journal of Business Research 170.

122 Mark Coulson and others, 'Real Feelings for Virtual People: Emotional Attachments and Interpersonal Attraction in Video Games.' (2012) 1 Psychology of Popular Media Culture 176.

123 Ruud Hortensius, Felix Hekele and Emily Cross, 'The Perception of Emotion in Artificial Agents' (2018) 10 IEEE Transactions on Cognitive and Developmental Systems 852.

124 Matija Franklin, 'Virtual Spillover of Preferences and Behavior from Extended Reality', *CHI Conference on Human Factors in Computing Systems* (2022).

riences may also lead to dissociation from physical and social environments, with users believing that certain tasks performed virtually have the same real-life consequences.[125] While this is a known complication of using VR for '*positive transfer effect*' in psychotherapy,[126] it may lead to dangerous results in uncontrolled consumer settings.

4. Broader impact on end-users

The preceding discussions demonstrate that AR/VR devices can worsen end-user vulnerabilities and facilitate newer vulnerabilities. While such harms remain largely theoretical, a recurring prominent concern is the 'manipulation of the mind'.[127] Such manipulative influence combines intentionality, asymmetry of outcome in favor of the manipulator, and non-transparency to violate users' autonomy.[128] These have also transcended into political discourses (for e.g., the Brexit and Cambridge Analytica situations[129]). In the consumer context, '*surveillance capitalism*' through our digital identities enables micro-targeting and behavioral modification, resulting in the loss of human will and independence.[130]

AR/VR's ability to identify and analyze our subconscious thoughts and emotions using neurological and behavioral tools could deepen these problems. For instance, hyper-personalization through AR/VR can lead to heightened exploitation of our existing vulnerabilities, which can erode human autonomy and attack individual agency[131] by making choices illusionary and using *sludging* to maneuver users' decisions, undermining our dignity and right to self-determination. Notably, these could intensify

125 Dhoya Snijders and others, 'Responsible VR. Protect Consumers in Virtual Reality' (Rathenau Instituut 2020) <https://www.rathenau.nl/sites/default/files/2020-03/Responsible%20VR.pdf> accessed 15 December 2022.

126 Mel Slater and others, 'The Ethics of Realism in Virtual and Augmented Reality' (2020) 1 Frontiers in Virtual Reality.

127 Yusef Al-Jarani, 'All Fun and (Mind) Games? Protecting Consumers from the Manipulative Harms of Interactive Virtual Reality' (2019) 2019 University of Illinois Journal of Law, Technology & Policy 299, 311.

128 Marcello Ienca, 'On Artificial Intelligence and Manipulation' (2023) 42 Topoi 833.

129 Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8 Internet Policy Review.

130 Shoshana Zuboff, 'Surveillance Capitalism' [2020] *Project Syndicate Quarterly*.

131 James J Cummings and Alexis Shore, 'All Too Real: A Typology of User Vulnerabilities in Extended Reality', *In Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality* (2022).

echo chambers, perpetuating increased inequality and discrimination by reinforcing stereotypes and biases.

Another concern is the power imbalance and information asymmetry: AR/VR devices assimilate nuanced data about preferences and perceptions more than traditional technologies. Assuming legally valid data collection, users may remain unaware of all uses of innocuous information due to the technology's nascency and associated information asymmetry. Thus, wider XR adoption could deepen the imbalance between platforms and users owing to more intrusive data processing and create arbitrary dependencies.[132] Since users typically believe that data collection is "*a series of single bounded transactions, where individual pieces of data are "given" to an organization in exchange for a specific service*",[133] the processing operations in AR/VR may create new layers of vulnerability for users.

Therefore, to sum up, AR/VR devices can amplify existing vulnerabilities in end-users through XR-specific choice architecture, dark patterns, targeted advertisements, and personalized marketing. Intrusive data collection mechanisms in AR/VR devices enable platforms to gain deeper insights into users' emotions and behavior, leading to newer vulnerabilities through techniques like memory falsification and cross-reality concerns. These can influence users' choices, preferences, and behaviors, resulting in manipulation, loss of autonomy and agency, and increased power imbalance between platforms and users.

III. Conclusion and input for policy remarks

The trajectory of AR/VR technologies' influence on end-users presents profound implications. As we have navigated through this chapter, it becomes abundantly clear that the Metaverse, with its promise of immersive experiences, holds inherent pitfalls, especially for persons in situations of vulnerability. The confluence of cutting-edge technology with behavioral science, facilitated by AR/VR devices, has the potential not just to shape but to reshape human behavior and cognition in unprecedented ways. The threats, ranging from manipulation of the mind to the undermining of human dignity and autonomy, are not merely speculative but have tangible instances rooted in recent political and societal discourses.

132 Gianclaudio Malgieri and Antonio Davola, 'Data-Powerful' (5 February 2022).
133 Fourberg and others (n 94) 31.

The dynamics of power and information, already skewed in the digital age, threaten to become even more imbalanced with the widespread adoption of AR/VR technologies. While users perceive data sharing as a bounded transaction, the depth and breadth of data assimilated by these devices blur such boundaries, introducing multifaceted situations of vulnerability. The very attributes that make AR/VR appealing—such as hyper-personalization—can be weaponized to erode individual agency, making choices more illusionary than ever.In essence, while AR/VR technologies stand as a remarkable testament to human innovation and creativity, they equally highlight the urgent need for ethical, legal, and societal introspection. It is incumbent upon policymakers, technologists, and society at large to collaboratively address these challenges, ensuring that the Metaverse remains an inclusive and empowering space, rather than one that magnifies situations of vulnerability. As we stand at the threshold of this new digital frontier, the decisions we make now will shape the future landscape of human interaction, autonomy, and dignity in the immersive digital universe.

Additionally, this discussion is directly relevant to the ongoing conversation surrounding the Digital Fairness Act that the European Commission is pursuing. As AR/VR technologies are increasingly integrated into consumer markets, their unique ability to collect, analyze, and manipulate user data at unprecedented levels of granularity poses new challenges for digital fairness. The concerns raised in this chapter about hyper-personalization, emotional manipulation, and memory falsification directly align with the Act's goals to prevent exploitation and ensure that users, especially vulnerable ones, are protected from undue influence and manipulation in the digital marketplace.

The importance of this alignment lies in the potential for AR/VR technologies to create environments where user autonomy and decision-making could be subtly compromised through techniques such as dark patterns and manipulative advertising. In the context of the Digital Fairness Act, these risks highlight the need for more robust protections that not only address traditional online platforms but also anticipate the novel ways immersive technologies can impact user behavior and cognition. By ensuring that the principles of fairness, transparency, and accountability extend to the Metaverse, the European Commission can safeguard against the deepening of existing vulnerabilities and the creation of new forms of exploitation, making the digital space more equitable for all users.

Vulnerability in the Age of Metaverse and Protection of the Rights of Users Under EU Law

Shabahang Arian

A. Metaverse: new frontier of digital life

Generally speaking, the metaverse represents an online three-dimensional space where individuals engage and interact as digital avatars in much the same way as they do in the real world.[1] Matthew Ball in his book "The Metaverse" refers to this space as an immersive, shared digital reality environment that offers the potential for exploration and customization by users, identical to the experience and freedoms they enjoy in the physical world. This digital space provides enormous opportunities for socialization, entertainment, shopping, other augmented reality services, and a variety forms of digital content.[2] Despite the current limitations in technology and infrastructure, preventing the development of immersive virtual worlds anytime soon, researchers are diligently examining the metaverse's potential and its impact of this transformative digital change.[3]

Although the metaverse is a relatively emerging technological frontier, it is not merely a singular innovation. In fact, this technology is developed and supported by a variety of diverse cutting-edge technologies including Extended Reality (XR), 5G connectivity, artificial intelligence (AI), the

1 Matthew Ball, 'The Metaverse: What It Is, Where to Find It, Who Will Build It, and Fortnite' MatthewBall.vc, [September 15, 2021b.], https://www.matthewball.vc/all/themetaverse. Accessed Sep 21, 2023. See also, Gideon Burrows, 'Your Life in the Metaverse: Everything You Need to Know About the Virtual Internet of Tomorrow'. [2022] J. Kim, 'Advertising in the Metaverse: Research Agenda' [2021] Journal of Interactive Advertising, *21*(3), 141–144.

2 Matthew Ball, 'The Metaverse: And How it Will Revolutionize Evertything'[2022]. Matthew Ball, 'Framework For The Metaverse' [2021a.] https://www.matthewball.vc/all/ forwardtothemetaverseprimer. Accessed Sep 21, 2023.

3 Ereni Markos & Lauren Labrecque, 'Blurring the Boundaries Between Real and Virtual: Consumption Experiences and the Self Concept in the Virtual World' [2009] Advances in Consumer Research, 36, 884–885. See also: J Brannon Barhorst et al., 'Blending the Real World and the Virtual World: Exploring the Role of Flow in Augmented Reality Experiences' [2021] Journal of Business Research, 122: 423-436.

Internet of Things (IoT), blockchain, cloud and edge computing, and the vast reservoir of data which powers the metaverse's dynamic landscape.[4] Enhanced by other technologies, the virtual reality and augmented reality provide immersive experiences that blur the boundaries between reality and virtual space. In this multifaceted technological ecosystem, the avatars serve as a bridge between individuals and their virtual selves, acting as digital twins that represent and interact on behalf of users.[5] A fundamental building block of the metaverse lies in the array of enabling devices including Mixed Reality (MR) and Virtual Reality (VR) headsets, haptic feedback systems, and cutting-edge environment rendering devices which through them, users can engage with and navigate these virtual spaces.[6] Real-time interactions between multiple users in virtual environments requires the use and adoption of these devices to both capture real-world objects and transmit the data.[7]

Moreover, the virtual-reality environments offer an unparalleled richness compared to traditional 2D media. This richness extends beyond mere social cues in the forms of text and audio message but also encompassing multidimensional visual elements and haptic sensations.[8] To fully immerse in the VR/AR experience, users must rely on specialized equipment, such as virtual reality headsets or wearable haptic gloves. For instance, Apple Vision Pro, Apple's latest innovation, is a wearable face computer that without any keyboard, mouse or touch, delivers the high-resolution displays directly to the user's eyes through eye tracking and gestures.[9] Another facet of this technological revolution is the use of VR haptic gloves which enable

4 Lik-Hang Lee et al., 'All One Needs to Know About Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda' [2021a]. https://doi.org/10.48550/ arXiv.2110.05352

5 Yogesh K. Dwivedi et al., 'Metaverse Beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy' [2022] International Journal of Information Management, 66, Article 102542.

6 Yassine Jadil, Nripendra Rana, & Yogesh Kumar Dwivedi, 'A Meta-Analysis of the UTAUT Model in the Mobile Banking Literature: The Moderating Role of Sample Size and Culture' [2021] Journal of Business Research, 132, 354–372.

7 Intel., 'Powering the Metaverse' [2021] https://www.intel.com/conten t/www/us/en/newsroom/opinion/powering-metaverse.html. Accessed Sep 21, 2023

8 Ralph Schroeder 'Social Interaction in Virtual Environments: Key Issues, Common Themes, and A Framework for Research'. In Ralph Schroeder (Ed.), 'The Social Life of Avatars' [Springer 2002]1-18.

9 Joshua Gans & Abhishek Nagaraj, 'What is Apple's Vision Pro Really For?' [2023] Harvard Business Review.https://hbr.org/2023/06/what-is-apples-vision-pro-really-for. Accessed Sep 21, 2023.

users to interact with virtual objects and surfaces in a natural and realistic manner. These gloves can effectively track the user's hand movements and can apply forces, textures, and even thermal cues to the user's skin.[10] In particular, the Emerge Wave-1 device, developed by a California-based tech company, facilitates the sense of touch in the metaverse and fosters emotional connections among metaverse participants.[11] This tabletop panel uses ultrasound waves to map virtual objects that they can see through virtual headsets and convert this into the feeling of touch through a technology called haptic feedback in order to provide a more realistic experience.[12] In this next-generation digital frontier, traditional forms of interaction, such as typing and tapping, are being replaced by a variety of sensory devices. With the use of headsets and a variety of sensory gadgets, users can constantly communicate with their friends and family.

These AR and VR technological advancements suggest that the metaverse is no longer a science fiction concept but rather is on the verge of becoming an integral part of digital experience. Thus, it is therefore expected that in the near future, the Metaverse will serve as a convergence point between the physical and digital worlds, allowing users to seamlessly navigate between the two, for a variety of purposes such as work, education and training, health care, exploration of personal interests, and vibrant social interactions.[13]Due to an embodied Internet, the metaverse offers a digital space in which users can experience an enhanced sense of presence and a new dimension of online interaction, more similar to real-life experiences.[14]

With its novel, unprecedented sensory experiences, this technology will transform the engagement in digital sphere in a radical way. As a result of this expansive technological domain, every aspect of our lives, including the services we engage with, and the information and content we access

10 Qi, Jiaming et al., 'HaptGlove—Untethered Pneumatic Glove for Multimode Haptic Feedback in Reality–Virtuality Continuum' [2023] Advanced Science. 10.1002/advs.202301044.

11 Emerge Wave 1. https://emerge.io/ Accessed Sep 21, 2023.

12 Victoria Masterson, 'Feel the Metaverse with Your Bare Hands- Using Ultrasonic Waves' [2022] https://www.weforum.org/agenda/2022/05/metaverse-vr-ultrasonic-tech-emerge/ Accessed Sep 21, 2023.

13 Dimitrios Buhalis, Daniel Leung, Michael Lin, 'Metaverse as a Disruptive Technology Revolutionising Tourism Management and Marketing' [2023], Tourism Management, Vol. 97, 104724.

14 Nick Clegg, 'Making the Metaverse: What It Is, How It Will Be Built, and Why It Matters' [2022] https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04. Accessed Sep 21, 2023.

to, can be intricately mediated by this new digital space. This emerging technology has also a profound impact on our social connection, how we interact with others, the friendships we form, and the new digital manners that we engage in the social interactions.

Once fully built, this emerging digital space will have a legal impact on rights of users. with the range of cutting-edge technological capabilities, the metaverse holds the potential to create new opportunities for both present and future societies but it can also introduce contradictions and vulnerabilities, resulting in unanticipated risks, challenges and backlash. Thus, the Metaverse, like any other technological advancements, while improves our digital experiences, it also exposes consumers to new forms of vulnerability. A lack of engagement with regard to addressing the risks posed by the Metaverse exacerbates the scale of the challenges, vulnerabilities, and abuses arising from this emerging digital interaction. Therefore, it is crucial to address the potential risks and vulnerabilities that users may encounter as a result of interacting in the metaverse and to safeguard the rights of users at this early stage of Metaverse development.

B. Metaverse can change marketing and online shopping experience

As the Metaverse continues to evolve, provides marketers new opportunities for marketing and advertising. With users becoming increasingly engaged and spending more time in the metaverse, opportunities for brand promotion and consumer interactions in an entirely distinctive ways will be multiplying.

Research in the field of marketing indicates that various Extended Reality (XR) technologies, including virtual reality (VR), augmented reality (AR), and mixed reality (MR), hold substantial potential as effective marketing tools. These technologies create consumer experiences akin to physical stores.[15] Contrary to traditional online stores, in the metaverse, companies would have virtual stores instead of traditional websites where customers' avatars would be able to browse virtual shops, enjoy hyper-vir-

15 Mariano Alcaniz, Enrique Bigne, and Jaime Guixeres, 'Virtual Reality in Marketing: A Framework, Review, and Research Agenda' [2019] Frontiers in Psychology. Vol. 10. https://doi.org/10.3389/fpsyg.2019.01530. See also: Yogesh Kumar Dwivedi et al., 'Metaverse Marketing: How the Metaverse Will Shape the Future of Consumer Research and Practice[2023] Psychology & Marketing 40 (4), 750-776.

tual conversations with assistants, try on clothing or accessories, and purchase through virtual transactions. [16] Several retailers, such as Adidas, have already introduced features like Virtual Fitting Rooms (VFR), enabling consumers to "try on" clothing virtually before making online purchases in this shared space. The companies such as IKEA, for instance, has released an augmented reality catalog app, enabling customers to preview furniture in their homes before purchasing it.[17] Many global firms, including J.P. Morgan[18], luxury brands like Gucci and Ralph Lauren[19], and hotel groups like CitizenM and EV Hotel Corporation[20], have started investing in the Metaverse. They are establishing virtual branches, selling digital products, and even developing virtual hotels.

As a result, brands can open fully immersive virtual stores in the Metaverse, eroding physical boundaries and engaging a broad spectrum of audience on a global scale in highly compelling ways. The additional advantage of commerce in the metaverse can also be related to AI personalization. By utilizing AI algorithms to interpret user interactions, businesses in the metaverse can customize stores or products in real time in order to enhance the shopping experience of their customers. These immersive experiences have the potential to use data collected in virtual environments to tailor recommendations and offers to targeted consumers and create powerful emotional connections between consumers and brands.[21] As a result, it is

16 Miklos Savary, 'The Metaverse: TV if the Future?' [2008] *Harvard Business Review*, *86*(2), 30. Oliver James Scholten et al., 'Ethereum Crypto-Games: Mechanics, Prevalence and Gambling Similarities' [2019] CHI PLAY '19: Proceedings of the Annual Symposium on Computer-Human Interaction in Play, 379-389. Nannan Xi, & Juho Hamari, 'Shopping in Virtual Reality" A Literature Review and Future Agenda' [2021] Journal of Business Research, 134(1) 37–58.

17 Luke Soon, 'The Way of the Metaverse Enhance Human Experience' [2023], https://www.linkedin.com/pulse/way-metaverse-enhance-human-experience-luke-soon/?trk=pulse-article_more-articles_related-content-card . Accessed Sep 21, 2023.

18 Ron Shevlin, 'JPMorgan Opens a Bank Branch In The Metaverse' [2022], https://www.forbes.com/sites/ronshevlin/2022/02/16/jpmorgan-opens-a-bank-bra nch-in-the-metaverse-but-its-not-for-what-you-think-its-for/?sh=9e1cf2c158d3. Accessed Sep 21, 2023.

19 Queenie Wong, 'Shopping in the Metaverse Could Be More Fun Than You Think' [2022], https://www.cnet.com/tech/computing/features/shopping-in-the-metaverse-could-be-more-fun-than-you-think/. Accessed Sep 21, 2023.

20 Alicia Sheper & Will Speros, 'The Hotel Industry Enters the Metaverse' [2022]. https://hospitalitydesign.com/news/development-destinations/hotel-industry-nfts -metaverse/. Accessed Sep 21, 2023.

21 Ahmed Ismail, 'Virtual Shopping in The Metaverse: How Brand Engagement in Self-Concept Influence Brand Loyalty' [2023], 10.2139/ssrn.4494222.

more likely that consumers will engage with a brand when they perceive that it is aligned with their preferences.[22]

Moreover, the Metaverse enhances social interaction and togetherness, making it a key advantage for marketing. Human beings are inherently social, and the Metaverse provides a platform for shared experiences and social interactions. Joint consumption, spanning activities such as movie watching, gaming, event attendance, and shopping, is a multi-billion-dollar business, and the Metaverse aims to capture a significant share of this market.[23] Studies have shown that immersive virtual environments can enhance presence, enjoyment, realism, and synchrony among participants over time, offering numerous opportunities for interactive experiences like virtual events and product demonstrations.[24]

Consequently, as the Metaverse expands, there will be a profound shift in marketing in the metaverse as well, and therefore, digital advertising tools and techniques will undergo a fundamental transformation.[25] Metaverse marketing, in contrast to traditional advertising methods, is often perceived as non-intrusive, more interactive, and immersive, which can easily capture the attention of users and provide value to them. Two noteworthy marketing techniques are likely to play a significant role in marketing in the Metaverse:

I. Virtual product placement (VPPs)

There is a long history of product placement in cinema, exemplified by such iconic instances as Reese's Pieces in Steven Spielberg's 1982 masterpiece, "E.T. The Extra-Terrestrial".[26] The statistics indicate that this strategic

22 Shakeel Siddiqui & Darach Turley, 'Extending the Self in a Virtual World' [2022] in NA-Advances in Consumer Research. *Vol. 33* eds. Connie Pechmann and Linda Price, Duluth, MN: Association for Consumer Research, 647-648.

23 Thorsten Hennig-Thurau & Björn Ognibeni, 'Metaverse Marketing' [2022] NIM Marketing Intelligence Review. 14(2). 43-47.

24 Jeremy N. Bailenson et al., 'Transformed Social Interaction: Decoupling Representation from Behavior and Form in Collaborative Virtual Environments [2004] Presence Vol. 13(4), 428–441. https://doi.org/10.1162/1054746041944803.

25 Louis Rosenberg, 'Marketing in the Metaverse: A Fundamental Shift' [2022] https://futureofmarketinginstitute.com/marketing-in-the-metaverse-a-fundamental-shift/. Accessed Sep 21, 2023.

26 Charles Goldsmith 'Dubbing in Product Plugs: How "Spider-Man 2" made [2004] *Wall Street Journal*, B1.

collaboration not only contributed significantly to the movie's staggering $800 million box office earnings but also resulted in an increase of 85% in Reese's Pieces sales during the week immediately following the film's release. From a psychological perspective, the effectiveness of product placement and brand integration as non-traditional advertising methods lies in their ability to resonate with viewers on emotional, subconscious, and social validation levels.[27] These techniques are designed to exploit a natural inclination of human brain that tends to respond subconsciously to specific stimuli. In this way, by implicitly inserting a product into a movie or television program as a passive actor, without mentioning characters, viewers are likely to experience positive emotions, such as happiness or relaxation, associated with the product. [28] Thus, product placement serves as an effective marketing tool and increases the likelihood of the viewer purchasing the product in the future.[29]

In the Metaverse, advertisements will evolve into promotional elements and activities seamlessly integrated into immersive environments on behalf of sponsoring brands. These VPPs will be precisely tailored to individual users, ensuring that they encounter these promotional artifacts at specific moments and locations that are most relevant to them. The authenticity and seamlessness of VPPs within immersive worlds have the potential to deliver impactful advertising experiences. However, there is a need for vigilant regulation to prevent the abuse of VPPs, as they may become indistinguishable from authentic experiences, potentially deceiving users.

In the metaverse, Virtual Product Placement (VPP) entails the injection of simulated products, services, or activities into immersive environments, whether they are virtual or augmented. This virtual product placement is on behalf of paying sponsors and strategically placed in a manner that makes them visible solely to a specific and targeted audience, closely tailored to the user's unique characteristics such as age, location, prefer-

27 Chelsea Collins, 'The Psychology of Product Placement and Brand Integration'[2023] https://blog.hollywoodbranded.com/the-psychology-of-product-placement-and-brand-integration#:~:text=The%20human%20brain%20is%20wired,commercial%20for%20the%20same%20brand. Accessed Sep 21, 2023.

28 T. Wasserman 'How to Measure Product Placement' [2005] Journal of Adweek. Vol. 46(3), 18-20.

29 Chelsea Collins, 'The Psychology of Product Placement and Brand Integration'[2023] https://blog.hollywoodbranded.com/the-psychology-of-product-placement-and-brand-integration#:~:text=The%20human%20brain%20is%20wired,commercial%20for%20the%20same%20brand. Accessed Sep 21, 2023.

ences, habits and profiles. This advertising method creates a compelling illusion, making the inserted elements appear as natural components of the immersive environment. [30] Nevertheless, as mentioned, this targeted VPP is unique to each user and is not replicated for others sharing the same surroundings. As such, this personalized advertising can sometimes blur the lines between what content is authentic within the metaverse and what constitutes simulated objects, artifacts, or content, potentially leading to user confusion.

II. Virtual spokes people (VSPs)

An alternative approach for marketing and advertising in the metaverse is known as Virtual Spokespeople, or VSPs. In this method, interactive AI-driven avatars as conduits for conveying persuasive promotional content are employed to discreetly encourage users to consider and purchase specific products promoted by these AI avatars on behalf of sponsor brands. These AI-powered conversational agents equipped with a profound understanding of users' beliefs, interests, and behavioral patterns, enable to deliver persuasive messages fit with the users interests and aspirations.The presentation and demeanor of these AI-driven avatars are meticulously tailored by advanced AI algorithms, geared toward optimizing their impact on each individual user. Recent breakthroughs in Large Language Models (LLMs) and photorealistic avatars have rendered VSPs a viable and potentially pervasive tool within the metaverse.[31]

VSPs engage users through two distinct modes of interaction: passive observation and direct engagement. In the direct engagement approach, users directly interact with these AI-driven characters, engaging in dynamic conversations. Conversely, the passive method strategically positions two simulated spoken avatars in close proximity to users engrossed in conversation. During this exchange, the characters subtly introduce and discuss the sponsored brand, allowing users to overhear the discourse.[32] This

30 Louis Rosenberg, 'Marketing in the Metaverse: A Fundamental Shift' [2022] https://futureofmarketinginstitute.com/marketing-in-the-metaverse-a-fundamental-shift/ Accessed Sep 21, 2023.

31 Ibid.

32 Louis Rosenberg, 'The Metaverse Will Be Filled with Elves' TechCrunc 2022.https://techcrunch.com/2022/01/12/the- metaverse-will-be-filled-with-elves/ Accessed Sep 21, 2023.

advertising strategy leaves users pondering whether these individuals are ordinary users or virtual characters, adding an element of uncertainty to the metaverse experience artifacts, or content, potentially leading to users confusion.

C. Persuasion vs manipulation in the metaverse

Picture this scenario: A targeted user strolls down a virtual or augmented street filled with avatars and other objects. Suddenly, an avatar bearing a striking resemblance to his favorite celebrity approaches him while casually wearing a hoodie from the user's favorite brand. The link on the screen immediately appears which encourages the user to click on the hoodie and place the order.

Further along the path, two avatars engage in a conversation about the unique features of a brand-new laptop, prominently mentioning the specific brand. The user had recently been browsing the internet in order to obtain information regarding the purchase of a new laptop. AI-generated avatars are exclusively intended to target the user's attention and centered the conversation around his taste and preference. These avatars appear only on the user display and are hidden from the view of other participants. Different prices and products are also offered to different users in the same environment.

The user finds themselves perplexed, unable to distinguish which objects are authentic and which are AI-generated sopkespeople who are solely present for advertising purposes. The avatars engaging in conversation are equipped with real facial expressions and natural eye movements which makes it even more difficult to discern which is a real avatar and which is AI promotional avatars. Through AI and IoT technologies, the virtual space enhances the user's sensory experience by playing his favorite song in the background. The music playing happens to be a track from the user's favorite singer, a tune he had recently played. In this intricate web of experiences, determining whether a piece of content is promotional or non-promotional become a difficult task.

These examples illustrate the practice of nudging, in which subtle and even misleading tactics are employed to subliminally influence users' actions, primarily by targeting their "shallow cognitive processes", without

providing them with alternative choices.[33] There is the persuasive design business model which encourages the designers and developers to use all interfaces and tools of technology sometimes even at the developmental stage to nudge consumers in order to maximize their profits. Therefore, the design features and the choice architecture encourage users to follow certain path or "alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives." [34] In these situations, the companies self-consciously persuade users to change behaviors, make certain choices or take actions. By collecting data from users and employing sophisticated algorithms for analyzing the data, the emerging technologies now possess the ability to influence and persuade users more autonomously and strongly. As such, these technologies are often referred to as persuasive technologies. For instance, computers, originally designed for calculations, storage, and retrieval, have gradually evolved to include persuasive elements in their design. [35] Consequently, Captology (Computers as Persuasive Technologies) will be used by companies as a deliberate technique in the metaverse for the purpose of persuasion. This term refers to a set of methods and techniques used by companies to change consumer attitudes and behaviors as a result of their use of technological tools. As such, all technological tools and interfaces should be designed so that they encourage people to purchase particular products or subscribe to special wellness programs.[36]

The synergy of Artificial Intelligence (AI) and the Internet of Things (IoT) offers marketers a valuable tool set for comprehending customer behaviors and preferences. This knowledge can be leveraged to craft personalized and highly effective strategies within the metaverse for nudge practices and personalized marketing. [37] As a result of the introduction of marketing automation, facilitated by AI, marketers are able to increase

33 Paul Kuyer & Bert Gordijn, 'Nudge in Perspective: A Systematic Literature Review on The Ethical Issues with Nudging' [2023] Rationality and Society, *35*(2), 191–230, 192.

34 Richard Thaler & Cass R. Sunstein, 'Nudge: Improving Decisions About Health, Wealth and Happiness' [2008] Yale University Press, 6.

35 Brian Jeffrey Fogg, 'Persuasive Technology: Using Computers to Change What We Think and Do' [2003] Morgan Kaufmann Publishers, 1.

36 Ibid. 16-17.

37 Bharati Rathore, 'Virtual Consumerism an Exploration of E-Commerce in the Metaverse' [2017] International Journal of New Media Studies, 4(2), 61-69. Michael Rüßmann e al., 'Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries' [2015] Boston Consulting Group, 9.

precision and the effectiveness of their advertisements with less manual intervention. Nevertheless, this business model sometimes goes beyond personalization, and AI is poised to propel hyper-personalization, not only by suggesting purchases based on historical behaviors but by foreseeing needs before customers themselves consciously recognize them.[38]

D. Layers of vulnerability in the metaverse

Nonetheless, these persuasive techniques can potentially give rise to novel forms of deceptive strategies and manipulation within the metaverse. The metaverse heavily relies on artificial intelligence (AI) for various functions, including content creation, content analysis, data analysis, AI-driven voice navigation, speech processing, and overall social interactions involving computer vision.[39] As a result of the interaction with virtual or augmented reality environments, consumers will face different dimensions of vulnerability.

The primary vulnerability of consumers lies in the fact that the metaverse confuses users as to whether they are interacting with AI-driven avatars or authentic individuals. In general, businesses can utilize a variety of manipulation techniques to persuade consumers in 3D immersive spaces, compared to traditional 2D online marketing. Further, with the recent advancements in Conversational AI, exemplified by systems such as ChatGPT and LaMDA, it is likely that these conversational AI agents to be deployed in the metaverse in the near future. A key purpose of these AI interactive agents is to engage the target audience in a real-time dialog with predatory agents that can skillfully persuade them to purchase particular products or trick them into disclosing sensitive personal information. This can become even more deceptive when the industry uses simulated avatars with real-time voice and photorealistic digital personas that see, move, and express like real individuals, while in reality, they are controlled by AI.[40]

38 Louis Rosenberg, 'The Manipulation Problem: Conversational AI as a Threat to Epistemic Agency' [2023] Conference: Generative AI and HCI Workshop CHI 2023 (GenAICHI 2023).

39 Uptal Chakraborty, 'Metaverse and Web3: A Beginner's Guide: A Digital Space' [2022] BPB Publications.

40 Louis Rosenberg, 'The Manipulation Problem: Conversational AI as a Threat to Epistemic Agency' [2023]. Conference: Generative AI and HCI Workshop CHI 2023

The second reason for the high level of vulnerability of consumers in the metaverse is related to large quantities of detailed information about the users that will be exposed during their interactions in the metaverse. In fact, the convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) plays a pivotal role in shaping the metaverse. As a result of the IoT's vast network of sensors and devices, companies are able to collect a wide range of metaverse data and meta-data in real-time. For example, a smart device installed in a home or store can be used to systematically monitor customer usage patterns, enabling businesses to fine-tune their services to meet the specific needs of each customer. As mentioned previously, there are numerous research prospects for enhancing sensory input within virtual worlds. To improve real-life experience by users, there is a need for enhancing visual, auditory, and tactile feedback in the metaverse, especially concerning avatar interactions and communication. The VR AR virtual interaction requires the use of many sensory technology equipment such as VR AR glasses, gloves, or other sensory devices beyond standard computing devices such as headphones, in order to create and experience senses including a sense of touching of virtual elements in the metaverse.[41]

As a result, the metaverse, along with its accompanying technological sensory tools, significantly increases the companies' ability to collect and analyze large amounts of behavioral, demographic, and biometric data from consumers for profiling and ultimately deploying these data for highly persuasive techniques tailored to each individual in a very personalized manner.

The collected data including the facial expressions, vocal inflections, avatars emotional reactions can algorithmically craft personalised advertising for each user, and trigger specific thoughts, feelings or interests in targeted user. Furthermore, large amounts of data generated in the metaverse can exploit the vulnerabilities of individuals, and companies exploit the vulnerabilities of consumers to maximize their profits. Therefore, the massive collection of data use to exploit people's interests and vulnerabilities particularly for purpose of marketing and targeting ads and selling more products and services.

(GenAICHI 2023). See also: Louis Rosenberg, 'The Metaverse Will Be Filled with Elves' TechCrunc 2022.

41 John Davis N. Dionisio, William G. Burns III & Richard Gilbert, '3D Virtual Worlds And The Metaverse: Current Status And Future Possibilities' [2013] ACM Computing Surveys 45, 3, Article 34, 38. DOI: http://dx.doi.org/10.1145/2480741.2480751, 34:15.

E. Protection of users in the metaverse under EU law

Nevertheless, the vulnerability of consumers should not be left unprotected. As a result, legal frameworks have been meticulously crafted so as to protect and uphold the rights of consumers in relation to the goods and services they receive. In order to establish a metaverse environment characterized by fairness and legal integrity, particularly within the marketing sphere, it is essential to meet the challenges inherent to this emerging digital landscape. In Europe, a number of robust and well-developed laws are in place to protect consumers against unfair business practices. These regulations cover a wide range of issues related to dark patterns, deceptive design, manipulative marketing tactics, invasions of privacy, unlawful data collection, exploitation of vulnerability through personalized marketing, and user's consent-related matters.

The purpose of this section is to shed light on the pivotal role that EU regulatory laws can play in preventing and mitigating unfair commercial practices and misconduct in the metaverse and analyze the legal dimensions of consumer vulnerability within this digital frontier. Accordingly, the article will investigate whether the existing EU legal frameworks can effectively tackle the challenges associated with the metaverse or if there remain regulatory voids that require further scrutiny, attention and resolution.

I. EU Data Protection Law and profiling

The emergence of metaverse technology will present a profound challenge concerning data and data protection. The metaverse relies heavily on technologies such as eye tracking, facial expression tracking, and emotional and behavioral monitoring, enabling extensive users surveillance. As a result, the metaverse, by its very nature, introduces novel categories of personal data, including facial expressions and avatars gestures and reactions, to data processing considerations[42] while simultaneously intensifying data gathering, especially concerning users' behavioral, emotional, biometric, and demographic aspects.

42 Leanne Mostert, 'Legal Issues in The Metaverse', Webber Wentzel. https://www.webberwentzel.com/News/Documents/2022/webber-wentzel-metaverse-part-1.pdf. Accessed 21 Sep 2023.

Metaverse service providers have inherent access to the actions, interactions, and communications of users through avatars in the metaverse. Companies may employ sophisticated advertising algorithms that are capable of monitoring personal characteristics in real-time. These traits include not only facial expressions, vocal inflections, and posture, but also physiological responses, such as heart rate and pupil dilation as well as emotional and psychological reactions often captured through wearable devices. This technological space significantly facilitates comprehensive consumer monitoring by companies, making it both easier and more feasible than ever before. This massive data collection enables companies to offer personalized communication[43] directly to the specific recipient[44] based on behavioral targeting and audience particular traits, hobbies, interests, behaviors, beliefs, intentions and shopping history, time of day, location, weather.[45]

In many instances, user data enables companies to offer different price ranges for the same product or service to specific groups of consumers based on their regions, age, affiliations, and more. Moreover, service providers and companies can monitor targeted consumers' browsing behaviors in the metaverse to determine if the user fits the "affluent customer" or "budget-conscious" profile. [46] Due to this, the information collected and inferred by behavioral tracking tools directly influences the prices.

Therefore, engaging in metaverse activities often involves the disclosure of substantial amount of personal data including what users do, see, say, feel and even touch in the metaverse.[47] It is clear that extensive data collection, coupled with emerging technologies such as IoT, AI, and machine learning has significantly elevated the metaverse's capacity for surveillance,

43 Alessandro Acquisti & Jens Grossklags, 'Privacy and Rationality in Individual Decision Making' [2005] IEEE Security and Privacy Magazine, 3(1), 26–33.

44 Sriram Kalyanaramanand & S. Shayam Sundar, 'The Psychological Appeal of Personalised Content in Web Portals: Does Customization Affect Attitudes and Behavior?' [2006] Journal of Communication, Vol. 56(1), 110-132.

45 Nadine Bol, et al., 'Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self- Disclosure Across Health, News, and Commerce Contexts' [2018] Journal of Computer-Mediated Communication, 23(6), 370–388.

46 Jakub Mikians et al., 'Detecting Price and Search Discrimination on the Internet' in HotNets Organizing Committee, Proceedings of the 11th ACM Workshop on Hot Topics in Networks (ACM 2012) 3-5.

47 Louis Rosenberg, 'Regulation of the Metaverse: A Roadmap' [2022] 6th International Conference on Virtual and Augmented Reality Simulations (ICVARS 2022), DOI: 10.1145/3546607.3546611.

data gathering, privacy intrusions, and potential risks of exploitation and manipulation.

Clearly, in contexts involving the collection and sharing of user data, the paramount concern is the protection of individuals from potential exploitation of their vulnerabilities. European law has firmly entrenched privacy as a fundamental right, initially within Article 8 of the European Convention on Human Rights (ECHR)[48] back in 1950. Subsequently, in 2000, this recognition was extended to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR)[49], with Article 8 of the CFR explicitly recognizing the right to personal data protection in the context of automatic processing, thus reinforcing this fundamental right.

> Taking a significant step forward, the EU introduced the General Data Protection Regulation (GDPR) in 2016[50], to meet the ever-increasing demand for information privacy within digital spaces, catering to the privacy expectations of individuals and consumers. The GDPR applies comprehensively to all forms of personal data processing. Within this regulatory framework, individuals, as data subjects, are empowered with the right to exercise control over their data, which must be duly respected by data controllers and all involved in data processing.

Utilizing user profiles derived from a wide range of data, businesses can include the name of the target, his/her demographic information and his/her browsing behaviors to reach particular members of the target audience.[51] Such data gathering, with advancements in artificial intelligence technology, leads to the problems of business manipulation and algorithmic discrimination. Using algorithmic decision making, companies offer discriminatory pricing based on online monitoring and profiling users. That can be included consideration of certain benefits and awards or increased pricing based on age, or particular health information, or unique user need

48 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms [1950]as amended by Protocols Nos. 11 and 14, ETS 5.

49 Charter of Fundamental Rights of European Union [2012] OJ C 326, 26.10.2012, 391–407.

50 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2019] OJ L119/1.

51 Edith G. Smit, Guda Van Noort, and Hilde Voorveld, 'Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe' [2014] Computers in Human Behavior, Vol. 32, 15-22.

and demand. As an example, companies may offer discounts to young people or increase their prices for older people, or by obtaining health information about the user, the company may offer a higher price since a specific drug related to the user's health issue is scarce in the geographical region where the user lives.

The companies often claim that such information collection about users allows them to provide personalized offers, recommendations, advertising, sales, and promotions to consumers[52] based on their needs, interests, and preferences.[53] However, in many circumstances, in such targeted advertising and marketing, the line between persuasion and manipulation is blurred.[54]

Personalization, as defined in the academic literature, involves the strategic creation, modification, and adaptation of content and distribution to optimize the fit with personal characteristics, interests, preferences, communication styles, and behaviors. In the context of the metaverse, personalization occurs in the form of personalized advertising which is created for an individual using information gathered through the individual's behaviors in the metaverse.[55] As such, personalization is a dynamic process that involves the interaction between companies and their consumers, the collection and processing of data, as well as the delivery of marketing outcomes. [56]

Therefore, three core elements can be understood in personalization: 'personal data' and 'automated processing' leading to 'various personalized decisions and outcomes' based on users' personal information and AI predictions and decisions. In analyzing whether data collection and processing by service providers in the metaverse are legitimate under EU laws, it is

52 Joanna Strycharz et al., 'Contrasting Perspectives – Practitioner's Viewpoint on Personalised Marketing Communication' [2019] European Journal of Marketing, 53(4), 635–660.

53 Sophie C. Boerman, Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius, 'Online Behavioral Advertising: A Literature Review and Research Agenda' [2017] Journal of Advertising, Vol. 46 No. 3, 363-376.

54 Joanna Strycharz & Bram Duivenvoorde, 'The Exploitation of Vulnerability Through Personalized Marketing Communication: Are Consumers Protected? [2021] Internet Policy Review, 10(4). Also see: Sandra Wachter 'Affinity Profiling and Discrimination By Association in Online Behavioral Advertising'[2021] *Berkeley Technology Law Journal*, *35*(2).

55 Jari Vesanen and Mika Raulas, 'Building Bridges for Personalisation: A Process Model for Marketing' [2006] Journal of Interactive Marketing' Vol. 20 No. 1, 5-20.

56 Jari Vesanen, 'What is Personalization? A Conceptual Framework' [2007] European Journal of Marketing, 41(5/6), 409–418. doi:10.1108/03090560710737534.

essential to address the question of what constitutes "personal information" in the metaverse and to what extent, "the collection" and subsequent "automated processing" of user information is permitted by EU regulations and rules. The the General Data Protection Regulation (GDPR) may apply to the metaverse as long as the data subject often represented by the avatar operator is located within the territorial boundaries of the European Union (EU) when the data undergoes processing.

To truly grasp the implications, it is imperative to first comprehend the expansive definition of personal data as outlined in Article 4(1) of the GDPR. This definition encapsulates any information, irrespective of nationality or place of residence, that pertains to an identified or identifiable natural person. It encompasses both objective data, such as name or address, and subjective data, which includes any information that evaluates, influences, or shapes an individuals' economic and social status or behavioral patterns, or potentially affecting their rights and interests. [57]

Crucially, the threshold for identifying an individual as 'identified' or 'identifiable' hinges upon their distinctiveness within a group of persons. In other words, an individual must be distinguishable from all other members of that group. Various means can facilitate this identification, ranging from traditional identifiers like names, addresses to the modern tools of surveillance, including IP addresses and cookies. [58] Notably, in the metaverse, personal data encompasses a diverse spectrum of information, transcending the confines of conventional data categories. For instance, elements such as facial expressions, eye movements, avatar gestures, and movements, when identifying a person, become part of the personal data context. According to recital 26 GDPR, to identify a person in the metaverse, 'all reasonable means' likely to be employed by the controller or by any other party to identify the person. Therefore, while data protection laws typically rely on identifiers such as names, phone numbers, and email addresses, the metaverse expands the boundaries and pushes the scope of personal data beyond conventional definitions. [59] As such, the personal data in metaverse may extend to include granular and inferential data such as facial expres-

57 A29WP, Opinion 4/2007 on the concept of personal data [2007] No. 01248/07/EN – WP 136, 6-8.

58 Ibid. 15-16.

59 Patrick Breyer v Bundesrepublik Deutschland [2016] European Court of Justice. Case C-582/14 Judgment of 19 October 2016, ECLI:EU:C:2016:779.

sions, eye movements, and avatar gestures as personal information.[60] As a result, the GDPR may need to encompass novel categories of personal data arising from interactions within the metaverse, which may be subject to processing by companies and service providers.

The General Data Protection Regulation (GDPR) lays down a comprehensive framework governing the processing of personal data, including within the ever-evolving landscape of the metaverse. Central to this framework is Article 4(2) of the GDPR, which casts a broad definition of what constitutes 'processing'. Article 4(2) defines processing as "any operation or set of operations performed on personal data, whether or not by automated means". These operations encompass a broad spectrum, ranging from the initial collection and recording of data to its subsequent organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, combination, restriction, erasure, or even its ultimate destruction.[61]

Principles outlined in Article 5(1)(a) of the GDPR further delineate the essential requirements for processing personal data within the metaverse. The Article acknowledges that in order for data controllers to process data of data subject, such data processing must be carried out lawfully, fairly, and in a transparent manner. In addition, Article 6 of the GDPR that sheds light on what constitutes lawful processing, highlighting a variety of conditions that must be met. Data controllers are thus faced with the legal obligation to identify and establish valid legal bases justifying their data processing activities. These bases serve as the cornerstone upon which lawful data processing hinges. The options delineated in Article 6 include data subject consent, necessity for the performance of a contract, or legitimate interests pursued by the controller or a third party, as stipulated in Article 6(1)(a), 6(1)(b), and 6(1)(f) of the GDPR, respectively. Each of these legal bases carries its own implications and requirements, demanding meticulous consideration and compliance within the metaverse's digital space.

With regard to legitimate interests, as clarified by the European Court of Justice, a threefold assessment is required. First and foremost, the data

60 Leanne Mostert, 'Legal Issues in The Metaverse', Webber Wentzel. https://www.webberwentzel.com/News/Documents/2022/webber-wentzel-metaverse-part-1.pdf. Accessed 21 Sep 2023.

61 Richard Steppe, 'Online Price Discrimination and Personal Data: A General Data Protection Regulation Perspective' [2017] *Computer Law & Security Review*, *33*(6), 768–785.

controller must unequivocally demonstrate the genuine legitimate interest. Secondly, the specific data under consideration must be integral to the achievement of these interests, requiring a stringent focus on data minimization and relevance. Finally, the rights of the data subject must not be superseded by the interests pursued by the data controller, striking a balance between individual privacy and legitimate objectives of organizations.[62]

In scenarios involving contractual processing, such as interactions in the metaverse where users and service providers engage in contractual relationships, it is imperative that the scope of data collection remains tightly aligned with the essential data necessary for fulfilling the contract's intended purpose. If the data is being collected for monetization or additional services, this should be clearly stated by data controllers since it is firmly grounded in separate legal bases that require transparency and compliance with data protection laws. To foster transparency and safeguard user privacy, stringent limitations should be imposed on the retention of data by platform providers within the metaverse. personal data should only be stored for the minimal duration necessary to facilitate the virtual experiences. This curtailment serves to significantly diminish the capacity of providers to use users detailed profiles over time. In addition, the transition from physical access to virtual access has transformed data vulnerabilities, necessitating stringent safeguards against unauthorized access particularly with respect to online infrastructure such as cloud storage.[63]

The additional requirement that takes center stage as a critical pillar of data protection, is the concept of consent as expounded in Articles 4(11) and 7 of the GDPR. To meet GDPR standards, consent must be freely given and unambiguous, with a clear and specific focus on each processing operation. Data subjects must receive adequate information to make informed decisions regarding the use of their data. As such, the platform providers in the metaverse must be duty-bound to communicate comprehensively with the public about the nature of data tracking within their metaverse platforms, including the precise data types monitored and the durations for which they are retained. For instance, users engaging in virtual or augmented worlds should receive overt notifications if VR and

62 See A29WP, *Opinion 06/2014 on 'The Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (2014) No. 844/ 14/EN – WP 217, 33.

63 Benjamin Edwards, Steven Hofmeyr, Stephanie Forrest 'Hype and Heavy Tails: A Closer Look at Data Breaches' [2016] *J. Cybersecurity*, 2, 3-14.

AR devices capture biometric data, such as eye movements, gestures, gaze or information regarding health and emotional conditions.

Nevertheless, the metaverse, by its very nature, blurs the line between reality and simulation, resulting in a realm imbued with ambiguity and fluidity. Users may engage with avatar-based influencers, participate in sponsored events, or partake in various metaverse activities, all of which can involve the collection of personal data for advertising and communication purposes. To protect the rights of metaverse users, robust and transparent privacy standards should be implemented, offering individuals a genuine, clear, and meaningful choice regarding the processing of their data.

In addition, a notable challenge arises from the opacity of many consent forms and privacy policies. What holds greater importance, however, is ensuring that individuals within the metaverse are afforded a genuine and easily comprehensible choice, which allows them to fully understand the reasons behind and methods employed for processing their data, as well as who is responsible for processing those data.[64] Nonetheless, the issue of aligning consent forms with legal requirements continues to raise concerns, particularly with regard to the crucial element of transparency. Lengthy, complex, and unclear documents, exacerbated by integration of simulated and real worlds in the metaverse can lead to confusion and uncertainty of users, impeding their ability to make informed and voluntary choices. In addition to these concerns, there are also the deceptive design patterns known as "dark patterns" that are frequently employed by service providers to mislead users into granting consent or sharing more personal data than they intended. As a result, this violates principles such as fairness, data minimization, and transparency, and is contrary to the principle of data protection by design. [65]

Also, consent must be 'specific' necessitating that the processing purpose must be clearly specified. This aligns with the 'purpose limitation' principle stipulating that personal data should be collected for explicit and legitimate purposes, without further incompatible processing. This means the extent of processing included in the purpose must not be overly broad that data subjects cannot evaluate compliance with data protection laws or discern for what purpose exactly the data is collecting. Therefore, upholding these

64 F. Zuiderveen Borgesius et al.,'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' [2017] *European Data Protection Law Review*, *3*(3), 353–368.

65 A29WP, *Opinion 15/2011 on the definition of consent* [2011] No. 01197/ 11/EN – WP 187.

standards ensures that data processing within the metaverse remains compliant, transparent, and respects the privacy rights of its diverse users.

As a result, price discrimination in the metaverse takes the form of personalized pricing which is rooted in online tracking and profiling consumers' behavior. According to Article 4(2) GDPR when companies use automated data processing to evaluate the economic status of individuals, this usage of algorithms for assessing the financial aspect of an individual falls within the scope of the profiling regulation. Profiling is classified as high-risk processing due to its potential impact on individuals' rights and invasion of privacy and confidentiality. Nevertheless, according to Article 22 of the GDPR the data subjects has the right to rectify data used for price discrimination and the right not to be subject to certain discriminatory pricing decisions. In such cases, the legal measures safeguard individuals' rights, allowing them to contest decisions, based solely on automated processing, including profiling.[66]

II. Manipulative business practice in the metaverse

In the burgeoning metaverse, users increasingly confront what are commonly referred to as 'dark patterns' within user interfaces. These manipulative tactics, often employed through conversational AI agents, pose unique threats to the agency of human users. Such practices deceive consumers by influencing their choices through deceptive design techniques, guiding them away from decisions that serve their best interests and instead aligning them with the commercial ends of companies. In order to personalize and persuade consumers for their products and services, firms frequently collect information about consumers' habits, preferences and interests through emerging technology. The metaverse introduces an additional level of vulnerability for consumers by offering a broad range of data for companies to gather and use for personalization and persuasion. While personalization offers advantages to both companies and consumers, it also harbors dangers. A dark design combined with an understanding of consumer vulnerability and emotional fragility may lead to misuse of this space by corporations. 'Persuasion profiling' is another method of abusing consumers, which involves companies identifying individual consumer mo-

66 F. Zuiderveen Borgesius & J. Poort, 'Online Price Discrimination and EU Data Privacy Law' [2017] *Journal of Consumer Policy*, *40*(3), 347–366.

tivations and interests and dynamically altering advertisements in real time to the consumer as a result.[67] In this way, firms can employ 'motivation analysis' by utilizing algorithms in order to take advantage of consumers' hidden vulnerabilities' in the decision-making process through exploitation of psychological and psychoanalytical methods.[68] In this way, companies leverage frailties and vulnerabilities for financial gain, adjusting prices for vulnerable demographics, exploiting local scarcities, or charging higher prices for consumers with specific health conditions. Consequently, data collected from users is leveraged against users by these companies, resulting in consumers' economic and privacy harm.[69]

Market manipulation is even more prevalent in the metaverse. As a result of the nature of metaverse, the line between the real and the simulated world can be blurred. In the metaverse, there are a number of manipulative tactics available in order to hiddenly shape one's choice architecture in order to influence his/her decisions without overtly coercing. By placing products within the environment or channel in which audiences interact, marketers can subliminally influence participants to purchase products. Alternatively by creating AI avatars customized to users' fantasies and aspirations and by triggering consumers' vulnerability and deceiving their perceptions, companies may influence consumers' choices and economic behavior. Dark pattern business marketing in the metaverse, therefore, may exert a covert influence on consumers' decision-making processes without their awareness. In 2019, the Council of Europe issued a Declaration on the Manipulative Capabilities of Algorithmic Processes, recognizing the growing capacity of contemporary machine learning tools "to predict choices" and "influence emotions and thoughts, and alter an anticipated course of action", sometimes in a subliminal manner. The potential dangers for democratic societies stemming from "employing such capacity to manipulate and control the manipulation not only economic choices, but also social and political behaviors" of individuals.[70] As a result of the integration

67 Maurits Kaptein and Dean Eckles, 'Selecting Effective Means to Any End: Futures and Ethics of Persuasion Profiling [2010], in Per Hasle at al. (eds), Persuasive Technology' Berlin Heidelberg: Springer, 82-93. Maurits Kaptein & Dean Eckles, Heterogeneity in the Effects of Online Persuasion, 26 J. INTERACTIVE MARKETING, [2012] 176, 176–88.

68 Ibid.

69 Ryan Calo, 'Digital Market Manipulation' [2014] 82 Geo. Wash. L. Rev. 995.

70 Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Process, (13 Feb 2019).

of AI, machine learning, and IoT technologies into the metaverse, this space is highly susceptible to AI manipulation and deceptive design. Nevertheless, regulation provides consumers with the means to safeguard themselves from such business practices, and it oversees market activities in order to determine what constitutes manipulation and what constitutes persuasion.

In this regard, a number of EU laws have the potential to safeguard individuals against these predatory business practices and the extensive data collection and data-driven technology used for consumer surveillance and detailed profiles in order to predict consumer behaviors.

For instance, both the Digital Markets Act and the Digital Services Act both have tackled the issue of dark patterns. The recent proposal of the European Union, the Digital Services Act (2022), prohibits companies and service providers from employing dark patterns "to deceive or nudge" recipients of their services "via the structure, design, or functionalities of the online interface or part thereof".[71] (DSA, Recital 39). These practices are defined as actions that "materially distort or impair, either purposefully or in effect, the ability of service recipients to make autonomous and informed choices or decisions", infringing upon users' fundamental rights, including the right to informed consent and freedom of choice (DSA, Recital 67).

Furthermore, Article 5(b) of Directive 2005/29/EC on Unfair Commercial Practices (UCPD) introduces a set of novel criteria for evaluating whether a commercial communication and practice is fair or not. These criteria are designed to take into account the impact of digital asymmetry on consumer decision-making processes. According to this article, commercial practices that significantly distort or have the potential to distort the economic behavior of the average consumer are prohibited. In Gut Springenheide GmbH, the Court established a benchmark for defining "the average consumer", which was described as a person who is "reasonably well-informed and reasonably circumspect and observant".This approach also has been adopted by UCPD in recital 18 which refers to average consumer as a person "who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors as

71 Amendments adopted by the European parliament on 20 January 2022 on the Proposal For a Regulation of the European Parliament and the Council on Single Market For Digital Services (Digital Service Act) and amending Directive 2000/31/EC(COM (2020)0825- C9-0418/2020-2020.

interpreted by the Court of Justice". [72]Also, a materially distorted economic behavior of the consumer is defined by Article 2(e) of the UCPD as the use of commercial practices that substantially impair the consumer's ability to make informed decisions, leading the consumer "to make transactions that they would not otherwise have made". Accordingly, Article 5(4) of the UCPD expressly prohibits aggressive commercial practices as unfair. A commercial practice is considered aggressive if, within its specific context, taking into account all relevant features and circumstances, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct concerning the product, thereby causing them, or likely to induce them, to make transactional decisions they would not otherwise have made (as defined in Article 8 of the UCPD)As a result, this provision prohibits certain aggressive pesuasive commercial practices in the metaverse, such as dark pattern design, setting and features that aggressively nudges consumers to click on the link for purchasing products or to subscribe the services.

Crucially, under Article 5(a) of the UCPD, businesses are held accountable for unfair marketing practices when they fail to meet "the requirements of professional diligence". This concept, in reference to Article 2(h) of the UCPD, denotes "the standard of specialized skill and care that traders are reasonably expected to exhibit toward consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity". This underscores that the assessment of the fairness or unfairness of business practices should be based not on how businesses "generally behave" but rather how they "ought to behave". [73]

The UCPD provides a comprehensive legal framework governing business practices that impact consumers' economic interests at various stages, from pre-contractual interactions through to post-contractual phases. The recent Commission notice on the interpretation and application of the UCPD reaffirms that the Directive encompasses dark patterns and dedicates a specific section (4.2.7) to elucidate how its pertinent provisions can be applied to data-driven business-to-consumer commercial practices. Moreover, it underscores that the UCPD can be effectively employed to challenge the fairness of such practices, including dark patterns, within the

72 Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurt [1998] Case C-210/96, ECLI: EU:C:1998:369.

73 Federico Galli, 'AI and Consumer Manipulation: What is the Role of EU Fair Marketing Law?'[2020] 35-64.

context of business-to-consumer commercial relationships. This, of course, is in addition to other regulatory instruments, such as the GDPR, that also play a role in regulating these practices. [74]

It must additionally be mentioned that Article 5.2.2 of the AI Act recognizes that other manipulative or exploitative practices facilitated by AI systems that is not directly addresses in the Act, can be addressed through existing data protection, consumer protection, and digital service legislations, in order to safeguard individuals' against risks of AI systems including protecting the right of users to make informed choices and decisions.

In general, UCPD safeguards consumers from dark patterns and misleading business practices. This includes all forms of AI manipulation whether AI systems present information to the consumers. AI systems programmed in the metaverse can intentionally omit or conceal certain important information about products and services. Many dark patterns often involve false information that induces consumers to make decisions they would not otherwise make. Therefore, it is essential to take into account the metaverse environment, interface, and features when assessing the presentation of information. Article 6 of the UCPD safeguards consumers against misleading practices, including those containing false information that deceives or is likely to deceive the average consumer. This provision underscores the importance of how information is presented to consumers, particularly relevant in the context of dark patterns. Similarly, Article 7 addresses misleading omissions, which become pertinent when dark patterns are used to withhold information from consumers, compelling them to make specific transactional decisions. This often occurs in scenarios like cost-traps, where consumers are led to believe that a digital service requires a one-time payment, only to discover later that subsequent payments are necessary to continue using the service.[75] According to the Commission's notice, the concept of "professional diligence" encompasses essential principles such as "honest market practice," "good faith," and "good market practice. These principles underscore the normative values that are pertinent to a specific field of business activity. Consequently, when businesses are in the process of designing the interface through which they will engage with

74 BEUC, '"Dark Patterns" and The EU Consumer Law ACQUIS; Recommendations for Better Enforcement and reform [2022], https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf., 6. Accessed Sep 21, 2023.

75 Ibid.

consumers, it becomes imperative for them to adhere to these principles.[76] In practical terms, this means that traders must take measures to ensure that consumers are not misled or unduly influenced by a user interface that guides them towards making specific decisions without affording them the opportunity to fully comprehend the implications of those decisions. In essence, any manipulative practice that significantly distorts or is likely to distort the economic behavior of an average or vulnerable consumer could potentially run afoul of the trader's professional diligence requirement.

Therefore,in the context of the metaverse, instead of employing subtle strategies like using silent characters, the traders and marketers can utilize AI-driven avatars that are virtually indistinguishable from real humans by average consumers and engage users in promotional conversations or showcasing virtual products. The content they display cannot be identifiable as advertising or non-advertising material and the entire presentation in the metaverse deceive and confuse users. If such deceptive design and settings effectively nudge consumers' behaviors, leading them to enter transactions they would not have otherwise chosen and compromise consumers' free will and infringe upon their right to make informed choices and give consent, all of the mentioned practices in the metaverse constitute unfair commercial practice under the UCPD. In this context, such business practices fall under the category of dark patterns and are explicitly prohibited under EU laws. This prohibition aims to protect consumers from manipulative tactics that undermine their autonomy and ability to make informed decisions in the digital environment.

III. Children as vulnerable users in the metaverse

Children are among the potential users of metaverse platforms, and they require special protection due to their age and credulity in the new digital metaverse space.

Children's participation in gaming and exposure to advertising in metaverse environments necessitates careful regulation. Augmented Reality (AR) and Virtual Reality (VR) spaces can exacerbate the vulnerabilities of children. Article 5(3) of the Unfair Commercial Practices Directive

76 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. 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 (2021), 127.

(UCPD) delineates an average vulnerable consumer as an individual particularly susceptible to specific practices or products due to mental or physical infirmity, age, or credulity. Consequently, robust measures must be implemented to shield children from targeted advertising designed to exploit their vulnerability. Moreover, the UCPD places an additional condition, stating that a commercial practice is unfair when the trader could reasonably be expected to foresee that the marketing practice might distort the economic behavior of the average vulnerable consumer. Courts generally consider a vulnerability reasonably foreseeable if the company engaged in the practice knew or should have known that it could negatively impact vulnerable users.

In this regard, data collection and advertising practices for children in metaverse spaces must adhere to a path of utmost clarity and transparency. Advertising content must be unambiguously distinguishable from non-advertising content, ensuring children can make informed distinctions. Strict prohibitions are imperative against manipulative techniques, such as in-game purchase inducements or privacy disclosures, facilitated through dark pattern designs or techniques. Article 5.2.2 of the AI Act, for example, prohibits AI practices that have a significant potential to manipulate individuals through subliminal techniques beyond their consciousness or exploit vulnerabilities in specific vulnerable groups, such as children or persons with disabilities, with the potential to cause psychological or physical harm.

Additionally, the extensive data collection within metaverse spaces, including personal information, raises profound concerns, especially concerning children. Studies have shown that children's awareness and understanding of data flows and processing are substantially influenced by the presence or absence of visual cues. Therefore, it is essential to provide clear cues to children regarding data collection and processing. The transition from our evolved cognitive systems, which rely on sensory cues for detecting threats in the physical environment, to online contexts where these cues are often absent or manipulated, can explain why privacy boundaries are different in the digital world. Unlike the physical world, where we can see, hear, or feel the presence of others, online environments lack these sensory cues, which makes it challenging to navigate privacy concerns.[77]

77 Kaiwen Sun, et al., 'They See You're a Girl If You Pick A Pink Robot With A Skirt: A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks' In *Proceedings of the 2021 chi conference on human factors in computing systems* [2021], 1-34.

Therefore, any entity collecting, using, sharing, or storing children's data must adhere to and comply with the stringent GDPR Privacy Protection requirements related to children. Under GDPR, if an advertiser or operator collects, uses, or discloses personal information from children under 16, they must first obtain verifiable parental consent before taking any such actions. It must be noted that under the GDPR[78] , article 6(1a), the processing of data can be lawful when the data subject has been given the consent for processing his/her information. With respect to the children and adolescents, GDPR implies that the minors above the age of 16 have the option of giving consent to the processing of their personal data; however, children under this age must have parental consent (GDPR, Art. 8). For data privacy, therefore, GDPR requires operators to provide clear and easily understandable privacy notices regarding the children data collection, use, and disclosure practices. Privacy practices should be communicated in a transparent manner, and prominently displayed so that parents can easily access them. The GDPR states that processing of minors' personal data by means of automated processing[79] (Art. 4.4 GPR) and behavioral advertising must comply with Articles 13 and 14 of the GDPR, be informed by minors and their parents, and be transparent about the legal basis for processing. Accordign to Article 13, the data controllers are obliged to provide informaiton related to the identity and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; or the legitimate interests pursued by the controller or by a third party, the recipients or categories of recipients of the personal data, the period of storing the data, etc., to the data subject when the personal information is collected and processed.

In summary, due to their age and credulity, children require special protection within the new digital metaverse space. Regulations are needed to govern children's gaming, advertising, and data privacy, with a focus

78 Regulation 2016/679/EU of the European Parliament and of the Council, of 27 April 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation - GDPR) [2016] OJ L119/1.

79 The Council of Europe Guidelines on Artificial Intelligence and Data Protection [2019]. See also: Alessandro Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection'[2016] 32 Comp. Law & Secur. Rev., 238 ff.

on transparency and safeguards to protect them from potential harm and manipulation.

F. Conclusions

In conclusion, the evolving digital landscape of the metaverse presents multifaceted challenges that demand continuous adaptation and cooperation between regulatory bodies, businesses, and technology providers. Ensuring fair business practices in the metaverse necessitates a comprehensive approach rooted in professional standards, good faith, and transparency. Subliminal advertising and manipulative tactics, such as dark patterns, undermine consumer trust and violate the right of users to make informed decisions.

The metaverse, is highly driven by sophisticated algorithms and extensive data collection. While personalization enhances user experiences and is valued by companies and consumers, it raises concerns about privacy invasion. Excessive data processing, fueled by big data, could lead to manipulative practices. In this complex terrain, the delicate balance between personalization and privacy must be maintained. Advanced advertising algorithms in the metaverse have reached a level where they can assess personal traits, including facial features, vocal inflictions, and even vital signs. This data profiling for advertising, if unregulated, risks exploiting users' profound personal information for the commercial interests of companies. While the General Data Protection Regulation (GDPR) has made significant progress in digital privacy, additional provisions may be needed to address emerging types of data and new methods of profiling in the metaverse. Stricter regulations are imperative to limit the scope and use of biometric, emotional and behavioral data for automated decision-making and profiling based on special personal data categories and minimizing the discriminatory effects.

In addition, in this digital space, distinguishing between manipulation and persuasion is paramount. The metaverse, driven by AI-powered nudging, poses significant risks. Marketers, utilizing AI- generated avatars for advertising, can subliminally connect products with consumers' fantasies and aspirations. A manipulation is often subtle, emotional, and involves subtly influencing decision-making without conscious awareness, usually for commercial purposes. Regulations must curtail manipulative practices that exploitation of consumer vulnerabilities, ensuring financial gains for

corporations do not occur through dark patterns and manipulative business practices especially with regard to new methods of Virtual Product Placement and Virtual SpokesPeople marketing.

In the metaverse, vulnerable users must be given special attention. Empowering and protecting vulnerable consumers, particularly children, against exploitative practices is essential. It is important for advertisers and operators to adhere to self-regulatory guidelines in order to engage young users responsibly. In summary, the metaverse relies heavily on advanced advertising algorithms and data collection techniques. Robust regulations are imperative to restrict the extensive data collection by companies and protect users from being exploited for promotional purposes. This includes avoiding subliminal advertising, clearly informing audiences of promotional content, and refraining from directly inciting purchases or nudging users toward transactions. Ongoing regulatory vigilance and technological adaptation are crucial to maintain fairness and legal standards for commercial practices in metaverse.

PART II
Conceptualizing Digital Vulnerability Beyond Consumer Law

Digital Vulnerability in a Post-Consumer Society. Subverting Paradigms?

Mateusz Grochowski[*]

A. Why digital vulnerability?

The concept of digital vulnerability[1] has recently been playing pivotal role in the EU discourse on consumer protection in the digital economy. Its emergence and rapid popularity arose primarily from shortcomings of the existing conceptual framework of consumer law, which made it difficult to incorporate a new group of problems instigated by the online market. This was due, first of all, to a highly formalized distinction between consumers and other market actors in EU law up to now. Secondly, in its classical design, EU consumer law was based on the average consumer benchmark,[2] and only to a small extent supplemented with the vulnerable consumer concept.[3] Both notions are intended to serve as standardized rubrics for application of those elements of the consumer law framework that require evaluation of behavioral determinants of consumer market conduct (such as awareness, knowledge and cognitive skills). This system has, however,

* The research leading to this chapter was supported by the National Science Center grant 2020/37/B/HS5/04212.

1 The concept of consumer vulnerability in this chapter builds on the seminal study by N. Helberger, *et al.*, 'Surveillance, consent and the vulnerable consumer. Regaining citizen agency in the information economy', in: Helberger *et al.*, *EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets* (BEUC: Brussels 2021); see also below section D.I. On further elaborations of this concept see e.g. Helberger *et al.*, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2021) 45 Journal of Consumer Policy 175; Micklitz *et al.*, 'Towards Digital Fairness' (2024) 13 Journal of European Consumer and Market Law 24.

2 On consumer law's overly broad reliance on the average consumer concept, see Esposito / Grochowski, The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration, 18 *European Review of Contract Law* 1 (2022).

3 See also Leczykiewicz / Weatherill, The Images of Consumer in EU Law, *in* Leczykiewicz / Weatherill (eds.) The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law, Hart Publishing 2016, 7–11.

proven too stiff to acknowledge new sources of consumer harm brought about by the online economy.

The digital vulnerability idea emerged primarily to overcome the limitations of this system and to make consumer law more sensitive to new types of threats faced by consumers in the online realm.[4] Above all, it seeks to provide a coherent framework for new dimensions of consumer weakness[5] resulting from the growth of the data- and algorithm-based economy. Constructed with this idea in mind, digital vulnerability was embedded in the classical imaginary of the consumer as a market actor who pursues intrinsically economic goals. In this sense, digital vulnerability shares its conceptual roots with the other areas of EU consumer law. It was built on the implicit assumption that consumers' goals and interests can be expressed in terms of the value of goods they seek to accrue on the market. Consequently, consumer law's entire system, including open-ended standards (such as good faith) and evaluation benchmarks (such as the average consumer model), have been calibrated for consumers as market actors who pursue economic goals in classical terms.

Over time this picture was partly altered by acknowledging that consumer interest and consumer harm may include also non-economic values such as satisfaction and other emotions.[6] Nonetheless, EU consumer law has never developed a systematic framework for including non-economic interests and non-economic harm. The expansion of the digital economy made this deficit particularly vivid and troublesome. Although the existing structures of EU consumer law have not proven defenseless in this regard, the lack of an underlying conceptual framework turned this exercise into a game of hide-and-seek. The early attempts to grapple with non-economic consumer interests resorted primarily to general tools such as the UCTD (Unfair Contract Terms Directive)[7] coupled with fundamental rights (espe-

4 For further discussion on the conceptual genealogy of digital vulnerability, see Grochowski, Digital vulnerability – intellectual origins, *in* Grundmann / Sirena (eds.) European Contract Law and Future Challenges Intersentia 2024 (forthcoming).

5 On various ways of understanding vulnerability in the digital consumer economy, see also OECD, *Consumer Vulnerability in the Digital Age*, OECD Digital Economy Papers, No. 355, June 2023, 12–14 and Galli, Algorithmic marketing and EU law on unfair commercial practices, Springer 2022, 188–192.

6 See e.g. E. Illouz, Emotions as Commodities. Capitalism, Consumption and Authenticity, Routledge 2017.

7 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34.

cially freedom of speech)[8] as a benchmark for understanding the essence of consumer detriment. The recourse to fundamental right was, however, not supported with any deeper concept of consumer weakness in the non-economic realm. The enactment of the DSA (Digital Services Act)[9] further amplified this problem, posing a threat of splitting consumer protection online into two worlds that cannot communicate with each other.

These shortcomings call for a more in-depth consideration of the place and role of non-economic interests within the consumer weakness/vulnerability agenda.[10] The chapter takes up this query and delves into the question of how consumer law can accommodate the new consumption modalities in the digital economy.[11] The analysis proceeds in four steps. It sets out with an outline of the consumer concept up to now, paying special attention to the interplay between economic and non-economic consumer interests (section B). The argument proceeds towards new consumption paradigms in the online economy, explaining the challenge they pose for consumer interest and consumer harm (section C.I.). Against this background, the chapter also takes a critical look at the bottom-up strategies employed in response to the broader and more diverse array of consumer interests (section C.II.). Further, the analysis identifies the main traits of the digital vulnerability idea, explaining to what extent it overthrows the classical conceptualization of a consumer as a market participant (section D.I.). With this in mind, the chapter formulates an outline of the 'post-consumer digital vulnerability' concept (section D.II.) and proposes ways to integrate it with the general digital vulnerability framework into a coherent framework (section D.III.). The text concludes with a few remarks about the possible future trajectory for 'post-consumer digital vulnerability', taking into account the parallel system of protection emerging in EU regulation of online platforms (section E).

8 See section C.II.

9 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, OJ L 277, 27.10.2022, p. 1–102.

10 On the role of various forms of consumer vulnerability within the conceptual agenda of consumer law, Grochowski, Digital Vulnerability: Hopes and Disillusions (unpublished manuscript, on file with author).

11 The chapter develops selected thoughts outlined in my earlier editorial: Grochowski, Consumer Law for a Post-Consumer Society, 12 *Journal of European Consumer and Market Law* 1 (2023).

B. Open-edged economic imaginary

The conceptual roots of the modern consumer law framework date back to the turn of 1960s and 1970s, when a mounting mass consumption society drew policymaking attention to the protection of rights of non-professionals on the market. While in the US the idea of consumer protection was rooted in the idea of consumers who were state citizens and who, therefore, should be protected against harmful market practices,[12] the European approach developed rather as a spillover of the ordoliberal ideal, adopted as the cornerstone of the political economy in the post-war Western Europe.[13] The emerging consumer protection in Europe was based on the imaginary of a consumer market and consumer law typical for that era. It focused attention on individuals buying products and services to satisfy everyday personal needs, from purchasing a car to getting a candy in a store. The goods consumer sought on the market were seen through the prism of exchanging goods and services of measurable economic value for money.[14]

Expectedly, the accents in consumer protection were placed primarily on supporting autonomous and informed market choices and ensuring the proper quality of goods and services.[15] The core of consumer protection law that formed in this way encompassed typical situation where consumer decision-making might be hampered by the contractual circumstances (off-premises and distance contracts), product safety, and unfair terms; later it was supplemented by rules on sale agreements and on other more specific types of consumer contracts (such as timeshares and credit).[16] All these acts rested on the implicit premise that consumer protection meant a protection of economic interests understood along conventional lines – i.e. as a value that can be expressed in monetary terms (or at least that is directly relatable

12 Herrine, What Is Consumer Protection For?, 34 *Loyola Consumer Law Review*, 240 (2022).

13 Krämer, The Origins of Consumer Law and Policy at EU Level, *in* Micklitz (ed.), The Making of Consumer Law and Policy in Europe, Hart Publishing 2021, 13–19.

14 See also Olsen, Consumer Imaginaries, Political Visions and the Ordering of Modern Society *in* Micklitz (ed.), The Making of Consumer Law and Policy in Europe, Hart Publishing 2021, 278–284.

15 See also, more generally, Freedman, A Short History of Consumer Policy in the EU *in* Leczykiewicz / Weatherill (eds.) The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law, Hart Publishing 2016, 452–458.

16 Tonner, From the Kennedy Message to Full Harmonising Consumer Law Directives: A Retrospect, in Purnhagen / Rott, Varieties of European Economic Law and Regulation. Liber Amicorum for Hans Micklitz, Springer 2014, 701–704.

to a monetary measure). This imaginary has been intrinsic to European consumer law ever since. It directly informed, for instance, the structure of the unfairness test in the UCTD, where the benchmark of 'consumer detriment'[17] has been tacitly understood as economic harm,[18] i.e. the unfavourable quality(value)/price ratio. Such an understanding of interest and harm is ubiquitous in EU consumer law and forms the backbone of its agenda.[19] The same logic applied to the average and vulnerable consumer models used to benchmark basic consumer features (such as knowledge, awareness and gullibility).[20] Although these notions do not build on any clear assumptions as to transaction type – and they could apply across all market sectors – they have been implicitly shaped as models of human behaviour in the market settings where consumers exchange conventional commodities in the sense described above.[21]

Over time this structure of consumer law was gradually becoming more porous and capable of accommodating market situations and interests that did not necessarily fit into the picture of classically framed consumption. The instances of non-economic interests transcending into the main body of consumer law were, however, rather an exception, and they have never been put into a coherent conceptual framework (notwithstanding the question whether the deep heterogeneity of these cases makes such framework at all feasible). However, it is worth looking at the most remarkable

17 Article 3(1) UCTD.

18 See e.g. Rott, Unfair Contract Terms, *in* Twigg-Flesner (ed.), Research Handbook on EU Consumer and Contract Law, Edward Elgar 2016, 299–301. It must, however, be noted that a segment of scholarship argues for a more situation- and sector-specific approach towards consumer detriment in the meaning of the UCTD – see Micklitz, Unfair Terms in Consumer Contracts, *in* Reich *et al.*, European Consumer Law, Intersentia 2014, 148–149, with further references. If extended beyond the economic context, this idea could possibly serve as a point of reference for freedom of speech and other post-consumer commodities discussed below.

19 Siciliani *et al.*, Consumer Theories of Harm. An Economic Approach to Consumer Law Enforcement and Policy Making, Hart Publishing 2019, 109–136; Esposito / Sibony, In search of the theory of harm in EU consumer law: lessons from the consumer fitness check, *in* Mathis / Tor (eds.) Consumer law and economics, Springer 2021.

20 Article 5(3) of the directive 2005/29/EC of the European Parliament and of the Council 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, OJ L 149, 11.6.2005, p. 22–39.

21 See e.g. Esposito / Grochowski *supra* (fn. 2), at 6–15.

or conceptually challenging examples of such situations, as they mark a gradual shift from the traditional consumer world to the new territory that will be further[22] described as "post-consumer".

The earliest instance of a non-monetary perspective in consumer law (and perhaps the one most rooted in consumer law theory and practice) has been responsibility for substandard package travel services. Conceptualized for the first time in the ECJ *Leitner* judgment,[23] it became widely known as responsibility for a 'ruined holiday', eventually making its way into EU legislation.[24] The doctrine builds on the premise that the consumer interests embedded in a package travel service are by their nature hybrid and embrace not only purely economic values, but also emotions and experiences that a consumer sought to attain by purchasing a particular service. Consequently, consumers can obtain not only monetary compensation for the direct loss of economic value (e.g. when the purchased resort stay is cancelled), but also for the frustrated prospects for the positive feelings associated with this service (relatively: for the negative feelings triggered by particular unpleasantness).[25] Along similar lines, consumers can also be compensated for emotional discomfort caused by interruptions of air travel. Under the air passengers' rights regulation,[26] the core compensation in the event of the cancellation or delay of a flight consists of a lump sum payment, irrespective of the ticket price and other direct economic parameters.[27]

22 See section C.II.

23 Judgment of 12 March 2002, C-168/00, *Simone Leitner v TUI Deutschland GmbH & Co. KG*, ECLI:EU:C:2002:163.

24 Article 13 of the Package Travel Directive - Directive (EU) 2015/2302 of the European Parliament and of the Council of 25 November 2015 on package travel and linked travel arrangements, amending Regulation (EC) No 2006/2004 and Directive 2011/83/EU of the European Parliament and of the Council and repealing Council Directive 90/314/EEC, OJ L 326, 11.12.2015, p. 1–33.

25 On the essence of non-economic harm in tourist services, see e.g. Havu, Damages Liability for Non-material Harm in EU Case Law, 44 *European Law Review* 492 (2019).

26 Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91, OJ L 46, 17.2.2004, p. 1–8.

27 On immaterial harm against the backdrop of the 261/2004 Regulation, see also Karsten, Passengers, consumers, and travellers: The rise of passenger rights in EC transport law and its repercussions for Community consumer law and policy, 30 *Journal of Consumer Policy* 117, 132–133 (2007).

Non-economic perspectives have been growing in consumer law also in other ways, beyond the direct economic rationale. Most importantly, EU law has recognized that consumers may be interested not merely in obtaining certain services and goods, but also in subscribing to certain ethical or political values. The agenda that consumers most frequently want to adhere to and advance through their market choices pertains to the ethics of manufacturing certain goods (embedded especially in various manifestations of the 'fair trade' movement) or consuming them (regarding especially the environmental impact of certain commodities or the ways of using them).[28] Consumer law has become incrementally more sensitized to these issues. In selected cases the interests of consumers have already been protected when the commodity they purchased did not represent non-economic values declared for it. The most vivid instance so far has been 'Dieselgate', where consumers received redress[29] for untrue statements concerning the CO_2 emissions of diesel engines. The gist of this determination rested on the clear premise that consumer interests (in this case: the right to obtain a good that conforms with its declared specifics) also encompasses values that relate to the consumer's social or political perspectives. In other words, the higher emission rates did not in any way affect the functionality of a vehicle – and, hence, they did not shift the quality/price ratio for consumers. However, deceptive representations about the engines collided with consumer expectations about the impact the purchase and use of a car may have on the environment.

In terms of result, consumers who made the purchase with the hope of making a contribution to sustainability were in fact supporting the opposite outcome. The accents in this case were placed, hence, on the non-economic

28 Particularly telling in this regard has been the citizen-consumer notion that encapsulated the ideal of a market actor who takes responsibility for collective goods and values and follows them through her everyday market choices – see e.g. Porter, The Consumer Citizen, OUP 2020, 14–21; Davies, The European Consumer Citizen in Law and Policy, Palgrave Macmillan 2011; Barra *et al*., Citizens, consumers and sustainability: (Re)Framing environ- mental practice in an age of climate change, 21 *Global Environmental Change* 1224 (2011).

29 For the EU legal domain, this right was eventually identified by the CJEU in two judgments: of 14 July 2022, C-145/20, *DS v. Porsche Inter Auto and Volkswagen* (ECLI:EU:C:2022:572) and of 8 November 2022, C-873/19, *Deutsche Umwelthilfe eV v. Bundesrepublik Deutschland* (ECLI:EU:C:2022:857). On the importance of these cases for the development of consumer law, see also, for instance, Bertelli, The Dieselgate Returns at the CJEU: Lack of Conformity, EU Consumers' Rights and Responsibility, 31 *European Review of Private Law* 1221 (2023).

spheres of consumer motivation and consumer interest, rather than on the purely monetary ones.[30] The essence of consumer detriment in these situations should, hence, be understood as an undermining of one's conscience and attitudes rather than economic interests.[31] As opposed to the classical framework shared by competition and consumer law, where consumer harm is understood in terms of economic loss,[32] the instances discussed above draw attention towards harm to one's feelings and values – or in other terms, to 'identity harm'.[33] Following similar patterns, consumer law is deemed capable of protecting consumers also in other cases of false state-

30 Grochowski, European Consumer Law after the New Deal: A Tryptich, 39 Yearbook of European Law 387, 410–411 (2020).

31 In more particular instances, consumers may also be protected in terms of other values they want to pursue on the market. This pertains, for instance, to requirements concerning indications regarding the geographic origins of product. Such requirements protect not only the general consumer interest concerning awareness of the exact geographic pedigree of a good, but they may also have a further ramification: by providing consumers with clear information about the geographical origin of a product, they may indirectly protect consumers who do not want to purchase products of particular origin for ethical reasons. See, for instance, CJEU judgment of 12 November 2019, C-363/18, *Organisation juive européenne and Vignoble Psagot Ltd v Ministre de l'Économie et des Finances* (ECLI:EU:C:2019:954). As the Court observed in this case (para 53), 'the fact that a foodstuff comes from a settlement established in breach of the rules of international humanitarian law may be the subject of ethical assessments capable of influencing consumers' purchasing decisions, particularly since some of those rules constitute fundamental rules of international law.' Critical of this decision (including the CJEU's understanding of 'ethical considerations'), Kanevskaya, Misinterpreting Mislabelling: The Psagot Ruling (2019) 4 *European Papers* 763.

32 P. Siciliani *et al.*, *supra* (fn. 19), at 2–15.

33 The notion was advanced by Dadush, who defines 'identity harm' as 'the anguish experienced by a consumer who learns that her efforts to consume in line with her personal values have been undermined by a business's exaggerated or false promises about its wares.' The author's analysis of identity harm focuses on sustainability as a consumer value: 'identity harm arises when a consumer learns that a purchase made her unwittingly complicit in hurting another human being or the planet.' (Dadush, Identity Harm, 89 *University of Colorado Law Review* 863, 865 (2018)). Without a doubt, however, this conceptual framework can be extended mostly in its entirety to other instances where consumers are manipulated into market activity that contradicts other values they seek to vindicate with their purchase on the market.

ments about the way a good was produced (false 'fair trade' declarations[34]) and its impact on the environment ('greenwashing'[35]).

In all these instances, EU consumer law proved to be capable of embracing a broad spectrum of consumer interests, exceeding the directly economic considerations. In other terms, the framework consumer protection acknowledged in various ways the compound and heterogenous nature of consumption as a social and market phenomenon. At the same time, however, all the instances discussed above situate themselves on the margins of consumer law. They have been deemed to be rather exceptional anomalies in the consumer protection agenda rather than a part of its mainstream. Moreover, they remained separated from one another and have never led to a coherent agenda of non-economic interest and harm in consumer law. Over time, this situation has become increasingly ill-suited to grasp new phenomena emerging in the consumer market.

C. Beyond the economic framework

I. Digital post-consumption and consumer harm

The lack of a clearer understanding of the extent to which non-economic values (or to be more precise: values that cannot be expressed in monetary terms[36]) should be integrated into the array of consumer protection became particularly vivid over the past years, with exponential growth in the digital consumer economy. Specifically, the latter developed a broad range of services that cater only for emotions and social experiences, without providing individuals with 'consumable' goods in the classical sense. These services involve the acquisition of new experiences and emotions, the building of social links, and establishing channels to express one's views and attitudes.[37] None of these forms of market participation is without parallel in the earlier consumer economy (here it is sufficient to mention tourist

34 See e.g. Czarnezki *et al.*, Greenwashing and Self-Declared Seafood Ecolabels, 28 *Tulane Environmental Law Journal* 37 (2014).

35 See e.g. Spedicato, Deceptively Green: How the EU's Unfair Commercial Practices Directive Can Support Trademark Law in Combating Corporate Greenwashing, *in* Thouvenin *et al.* (eds.), Kreation Innovation Märkte – Creation Innovation Markets. Festschrift Retro M. Hilty, Springer: Berlin 2024.

36 See section B.

37 Grochowski, Consumer Law for a Post-Consumer Society, 12 *Journal of European Consumer and Market Law* 1 (2023).

services that to a great extent involved catering for emotions, experiences and social interactions). However, the current economy amplified these patterns to an unprecedented extent and surrounded them with complex structures of commodification and value extraction.

Commodities that give consumers access to experiences and feelings without involving a direct purchase are one of the components of the post-consumerist universe. The latter term took on a broad array of understandings in social and economic academic literature,[38] all of which, however, emphasize one crucial trait: in the post-consumer reality, individuals treat markets as a sphere for pursuing one's positive emotions,[39] social links[40] and personal growth[41] rather than as a realm simply for the acquisition of goods.[42] The digital economy to a great extent functions around these spheres of consumer motivation, responding to individuals and reflecting 'a growing interest in experiences, emotions and services, a revival of repairing, and the spread of leasing initiatives and sharing networks enabled by the internet'.[43]

This market strategy became the backbone of the social media sector.[44] Platforms crafted an utterly new set of consumer services, placing them-

38 For a review of existing theoretical accounts, see Cohen, Collective dissonance and the transition to post-consumerism, 52 Futures 42 (2013).

39 Pine / Gilmore, The experience economy, Harvard Business Review Press 2011, 3–7.

40 Becher / Dadush, Relationship as Product: Transacting in the Age of Loneliness, 2021 *University of Illinois Law Review* 1547 (2021).

41 Hayden / Wilson, Beyond-GDP indicators: changing the economic narrative for a post-consumer society? *in* Vergragt *et al.* (eds.), *Social Change and the Coming of Post-consumer Society. Theoretical Advances and Policy Implications*, Routledge 2017; Szejnwald Brown / Vergragt, From consumerism to wellbeing: toward a cultural transition?, 132 Journal of Cleaner Production 1 (2015); Cohen, The Decline and Fall of Consumer Society? Implications for Theories of Modernization, 2015 Global Modernization Review: New Discoveries and Theories Revisited 33 (2015).

42 Some expressions of non-material consumer interest mentioned in the previous section, such as the fair-trade and pro-environmental agenda, can clearly be labelled as post-consumerist in the currently discussed terms. On post-consumerism as a label for mobilization around collectivist market values and socially-sensitive attitudes towards consumption, see e.g. Schor, The new sharing economy: enacting the eco-habitus, *in* Vergragt *et al.* (eds.), Social Change and the Coming of Post-consumer Society. Theoretical Advances and Policy Implications, Routledge 2017; Soper, Other Pleasures: The Attractions of Post-consumerism, 2009 *Social Register* 115 (2009).

43 Trentmann, Empire of Things. How We Became a World of Consumers, from the Fifteenth Century to the Twenty–First, Harper Collins 2016, 682.

44 From the institutional perspective of EU law there can be no doubt that platform users qualify as consumers as long as they enter platforms for non-professional pur-

selves in the role of intermediaries in building and maintaining social relations. In so doing, the platforms gave rise to a new set of consumer interests, which could hardly be accommodated by the classical economic framework. Admittedly, contracts between users and social media platforms are not gratuitous and involve a certain degree of exchange, with personal data and consumer attention as the price for social services.[45]

Obviously, the new types of consumable assets and consumer values associated with them are not risk-free for consumers. The power structures that underly the digital consumer economy replicate in many regards dominance/weakness schemes from the brick-and-mortar market. Platforms create isolated social and market domains that are heavily self-regulated with limited impact of state governance. This market power of platforms manifests itself most vividly in shaping freedom of speech,[46] as well as in reconciling conflicts between free expression, privacy and other fundamental rights.[47] In all these regards platforms may misuse or abuse their power over users, harming their emotions and inter-personal liaisons, as well as frustrating expectations about the degree to which their personality and 'identity'[48] is protected by a platform.

From this vantage point, platforms can be considered as providers of a particular modality of consumer services – namely the 'speech infrastructures'[49] that allow platform users to follow their individual aspirations and

poses – see e.g. CJEU judgment of 25 January 2018, C-498/16, *Maximilian Schrems v Facebook Ireland Limited* (ECLI:EU:C:2018:37). The German case law mentioned in fn. 63–65 further confirms this unanimous viewpoint.

45 Langhanke / Schmidt–Kessel, Consumer Data as Consideration, 4 *Journal of European Consumer and Market Law* 218 (2015).

46 See e.g. Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 *Harvard Law Review* 1598 (2018).

47 On a general conceptual framework of platforms as suppliers of proportionality in the fundamental rights domain, Łakomiec, Public law and co-regulation. Influence of human rights discourse on internet platforms' standard of privacy protection, *in* Casarosa / Grochowski (eds.) Enforcing Private Regulation in the Platform Economy, Mohr Siebeck 2024 (forthcoming).

48 See section D.II.

49 The notion of 'infrastructure' is used here beyond its context in market regulation and public policy – see e.g. Zuckerman, The Case for Digital Public Infrastructure, Knight First Amendment Institute 2020; Hallinan, Civilizing infrastructure, 35 *Cultural Studies*, 707 (2021). In the discussion that follows, it is used as a synonym for a cluster of technological and private regulatory instruments set up by a platform to enable a particular sphere of user activity and to govern it.

values through social interactions.[50] From one side, growth of this market sector can be seen as a tenet of overwhelming commodification of private and social phenomena,[51] from privacy,[52] to attention,[53] to social relations[54] and emotions ('emodities').[55] From the other side, however, commodification should be seen as a two-sided phenomenon. It does not only involve extracting economic value of objects that have so far not been considered as belonging to the market realm;[56] it also concerns establishing a new type of a good or service that can be acquired by other market actors, such as consumers. In other words, in most instances commodification is inseparably intertwined with questions regarding the quality of goods and services emerging on the market.

In this way, commodification entails an immediate challenge for the legal framework of the market: How should we conceptualize the proper standard for the new market assets and how should we protect these who are 'passive' actors of commodification process, i.e. consumers and other market subjects? The social media sector has made this question particularly vivid in a few regards. One of them relates to privacy and extracting consumer data as a commodity.[57] Another is the psychological safety of services provided to consumers by social media platforms.[58] The third one – particularly relevant for 'post-consumer consumer law' – is the coherence between the quality of social media services, users' expectations and the objective quality standards.

50 See also Cohen, The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy, 31 *Philosophy and Technology* 213 (2017); Allmer, Critical Theory and Social Media. Between Emancipation and Commodification, Routledge 2015; Sion, Social Media-based Self-Expression: Narcissistic Performance, Public Adoration, and the Commodification of Reified Persona, 11 *Contemporary Readings in Law and Social Justice* 70 (2019).

51 Lobel, The Law of the Platform, 101 *Minnesota Law Review* 87, 90 (2016).

52 Schwartz, Property, Privacy, and Personal Data, 117 *Harvard Law Review* 2055, 2062 (2004).

53 Wu, Blind Spot: The Attention Economy and the Law, 82 *Antitrust Law Journal* 771 (2019).

54 Illouz, *supra* (fn. 6), at 5–8.

55 Benger Alauf / Illouz, Emotions in Consumer Studies, *in* Wherry / Woodward (eds.) The Oxford Handbook of Consumption, OUP 2019, 239.

56 Hermann, The Critique of Commodification. Contours of a Post-capitalist Society, OUP 2021, 20–39.

57 Kapczynski, The Law of Informational Capitalism, 129 *Yale Law Journal* 1460, 1498–1499 (2020).

58 See e.g. Bietti, The Data-Attention Imperative, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4729500

II. Deficits of the legal framework

Unsurprisingly, when confronted with the social media speech infrastructures, consumer law turned out to be ill-equipped to grasp the peculiarities of the consumer interests and consumer harm involved. Relying heavily on the classical (monetary) conceptualization of the consumer market,[59] the conventional legal framework proved mostly defenseless towards new modes of online consumption. The problem is visible already at the linguistic level. The conventional notions of a 'good' and 'service' can hardly be applied to non-economic commodities – such as freedom of expression or autonomy in establishing social relations – without a conceptual shift in their understanding. This dilemma can be easily traced to the language used in the existing policy and judicial accounts of the social media sector. While grappling with the interrelationship between the social media business model and consumer protection, one German court described the commodity in question as '"Facebook services" rendered under the platform-user contract'.[60] This notion was needed to conceptualize the platform/user relationship in the language of consumer law and to infuse it with a new notion of consumer harm. Similar conceptual tensions are typical for other commodities that cannot be directly defined within the classical economic framework of consumer law.

Attempts to address non-economic consumer interests resorted primarily to general tools such as the UCTD, which was invoked by courts as a benchmark in reviewing whether the particular clause in the platform's terms of service was unfair.[61] The economic components used in defining consumer interests and consumer harm were being replaced in this regard by fundamental rights.[62] In the social media sector, this concerned primarily shaping freedom of speech through content moderation[63] or through

59 See section B.

60 Landgericht Munich, judgment of 11 August 2018, 11 O 3129/18.

61 Lutzi, Plattformregulierung durch AGB-Kontrolle?, Verfassungsblog, 30 July 2021, https://verfassungsblog.de/facebook-agb-kontrolle/

62 Grochowski, From Contract Law to Online Speech Governance, Verfassungsblog, 18 May 2023, https://verfassungsblog.de/contract-speech.

63 See judgments of the German Supreme Court (*Bundesgerichtshof* – BGH) of 29 July 2021, III ZR 179/20 and III ZR 192/20 that questioned Facebook's speech moderation policy (suspension of users' account with reference to platform's Community Standards) as excessively limiting freedom of speech; see also Sprenger, Enforcing Put Backs in German and European Law, 72 *GRUR International* 933 (2023).

other acts of internal governance as done by a platform (such as the obligation imposed on users to present themselves online in a particular way[64]). In a more specific instance, the same logic was applied to review Facebook terms of service that denied the heirs of a deceased user access to her account.[65]

Fundamental rights served in these cases as a benchmark for determining whether the consumer service poses no harm to platform users – or, to put it in consumer law terms, whether it causes no consumer harm. The essence of this harm was defined, however, in specific terms as detriment to the sphere of a consumer's personal liberty, identity and freedom to express one's self. This conceptualization of harm was placed entirely beyond the area of economic considerations. Instead of identifying the particular market commodity or economic interests infringed by a platform, attention was primarily focused on the question whether – and to what extent – consumers were deprived of values protected as fundamental rights. Undeniably, this approach provides a convenient point of reference for handling consumer law disputes in the post-consumer realm. Reference to fundamental rights allowed courts to overcome other problematic issues related directly to defining consumers and their interest in the online economy. At the same time, however, the attempts in question have been too isolated to ground a satisfactory framework for the new types of consumer interests addressed in the platform economy.

D. Post-consumer vulnerability

I. Digital vulnerability: the overall origins

In the ways described earlier, the proliferation of post-consumer models raises a question regarding the effective protection of platform users in

64 See judgments of BGH of 27 January 2022 III ZR 3/21 and III ZR 4/21; see also Stadler / Franz, Keine Klarnamenpflicht bei Facebook, 75 *Neue Juristische Wochenschrift* 1282 (2022).

65 See judgment of BGH of 12 July 2018, III ZR 183/17; see also Wüsthof, Germany's Supreme Court Rules in Favour of Digital Inheritance, 7 Journal of European Consumer and Market Law 205 (2018). In this particular instance, the Court referred to the right of inheritance protected under Article 14(1) of the German Constitution (*Grundgesetz*).

the digital economy. As it was already said,[66] the existing notion of digital vulnerability builds on the premise that consumers involved in the online economy are exposed to specific risks stemming from this market environment. As opposed to the classical notion of consumer vulnerability (in its most developed form as embedded in UCPD), consumers are not digitally vulnerable due to intrinsic personal features distinguishing them from the other members of the group (such as age and health). The essence of vulnerability in question rests on the premise that architectural and relational[67] features of the digital market make consumers particularly prone to certain types of harm. In these terms, all humans carry certain degree of vulnerability,[68] which can be activated when they place themselves in the digital market environment.[69] As the authors of the study observe, 'digital vulnerability … results from power imbalances between consumers and sellers: consumer vulnerabilities can be identified and/or created because consumers interact with sellers within digital environments that can learn about them and be adapted accordingly. Given the data-driven nature of contemporary digital commercial practices, every consumer is dispositionally vulnerable to being profiled and targeted exploitatively.'[70]

In a nutshell, the concept of digital vulnerability is structured around two main building blocks: it relates either to the contracting process or to consumer data. In the first regard, consumers may be vulnerable especially due to their higher susceptibility to online manipulation (widely known under the catchphrase of 'dark patterns') and to new types of harm arising from new types of consumer products and services (including, for instance, digital market assistants[71] and other types of software merchandised as consumer commodities). In terms of data, consumer harm can result from infringements of privacy as such, as well as from the way their data is subsequently handled – especially by subjecting consumers to algorithmic decision-making (such as personalized advertising and price personaliza-

66 See section A.

67 For further discussion on the relational and architectural components in defining consumer vulnerability, see Helberger *et al.*, Surveillance, *supra* (fn. 1), at 18–23.

68 Dodsworth *et al.*, Editorial: Digital Vulnerability, 46 *Journal of Consumer Policy* 413 (2023).

69 On these two ways of defining consumer vulnerability, see also Riefa, Protecting Vulnerable Consumers in the Digital Single Market, 33 *European Business Law Review* 607, 610–614 (2022).

70 Helberger *et al.*, Surveillance, *supra* (fn. 1), at 25.

71 Van Loo, Digital Market Perfection, 117 *Michigan Law Review* 815 (2019).

tion). The core structure of digital vulnerability can, hence, be envisaged as follows:[72]

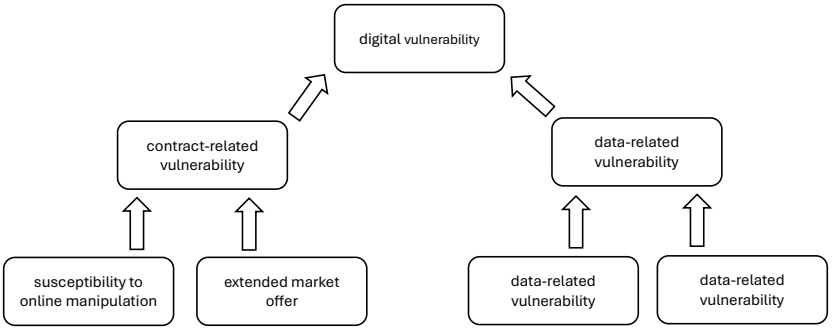


Fig. 1 – Digital vulnerability

Digital vulnerability, as with the entire conceptual structure of consumer law, rests heavily on the classical economic framing of market interests and harm. Although to some extent non-economic values (such as privacy[73]) are part and parcel of digital vulnerability, this is primarily spillover from the fact that those values have been already vastly commodified. In this way, digital vulnerability captures a relevant characteristic of the problems faced by consumers in the most typical parts of the online economy that involve purchasing goods and services in a traditional form.

II. The architecture of post-consumer vulnerability

The framework of digital vulnerability does not directly acknowledge that consumers' market aspirations do not always involve classical modes of consumption. In other terms, the concept of vulnerability can be reconsidered from the perspective of the post-consumer digital economy, including especially various amenities of the social media sector. Keeping in mind the earlier conclusions about the nature of consumer interests involved

72 This conceptual scheme of digital vulnerability is discussed in more detail in: Grochowski, *supra* (fn. 4).

73 Helberger *et al.*, Surveillance, *supra* (fn. 1), at 23–24; see also, generally, Malgieri, Vulnerability and Data Protection Law, OUP 2023.

in non-economic modes of consumption,[74] there is no doubt that by entering into contracts with online platforms and other providers of social experiences and emotions, consumers may expect a certain quality of such services. In most cases, the benchmark for evaluating this quality cannot be expressed in purely economic terms and requires other rubrics. Typically, the standard in question is formed at the intersection of general social practice and specific requirements of the online world.

Consumers may expect that the way certain services are delivered to them will correspond with the overall shape of this social interaction to the extent that it aligns with specificity of the online sphere. In this way, for instance, not all the statements admissible within the circle of family or friends are lawful in the specific context of the speech forum created by an online platform. With this in mind, the conceptual structure of the post-consumer side of digital vulnerability can be described with reference to two main parameters.

The first of them relates to the consumer's personal sphere and encompasses two main types of threats: the safety of information communicated to users and the risk that users will not be able to produce and share information. These notions describe two sides of consumer participation in non-economic online services.

On the passive end, consumers are exposed to information of various forms and content (such as a newsfeed on social media). They may, hence, reasonably expect that this information will respect certain minimal standards of directness and truthfulness. Understood in this way, information safety as a consumer standard prohibits, for instance, exposure to fake news (being both false as to content and deceptive as to its origins[75]) and to graphic content that may injure the feelings of unsuspecting users.[76] Certainly, not every meddling with information as done by a platform should

74 See the previous section.

75 Mathiesen, Fake News and the Limits of Freedom of Speech, *in* Fox / Saunders (eds.), Media Ethics, Free Speech, and the Requirements of Democracy, Routledge 2018.

76 Interestingly, the 2023 OECD report on digital consumer vulnerability counts fake news amongst instances of consumer vulnerability triggered by online transactions. It is not fully clear whether the authors of the report understood fake news merely from the transaction-related perspective (i.e. as deceptive statements intended to lure consumers into purchasing certain products) or whether they think of it also as a consumer issue per se. At any rate, however, certain fake news may also directly impact consumer purchasing behavior (which was the case, for instance, for untrue statements about Covid-19 treatment); OECD, *supra* (fn. 5), at 15–16.

be deemed a manifestation of consumer vulnerability.[77] For instance, curating the newsfeed with use of algorithms does not always lead to consumers being deprived of their informational autonomy or exploit their vulnerability. This may happen, however, if user data is misappropriated to produce individual user profiles, to apply dark patterns[78] or to commit other abuses of a platform's power in the process of personalization.[79]

On the active side, consumers seeking non-economic values on the digital market are usually interested in enjoying autonomy in expressing their views, abilities (e.g. sharing art created by themselves) and personality. The main component of this liberty encompasses freedom of speech, understood as both a fundamental right and as a benchmark for the quality of consumer services (see also below). Additionally, consumers may also expect that expression fora available to them online will provide not merely formal but also substantive self-expression autonomy – i.e. that they will be free of hate and other forms of violence that could otherwise deter users from expressing themselves in the way they intend to.[80] This domain of post-consumer digital vulnerability relates to the quality of services provided to consumers online. Taking social media platforms as an example, it is easy to illustrate this form of consumer susceptibility by comparing 'speech infrastructures' in the sense discussed above with the classical framework of compliance for consumer goods purchased in a sales agreement. When creating an account on a social media platform, consumers have a right to receive a service that will respect standards expressed both directly in the contract and inferred from social practice and reasonable consumer expectations.

These two components are crucial for our understanding of consumer vulnerability in the post-consumer context. As has been stated above, the essence of vulnerability rests in exposing sensitive areas of a consumer's self

77 Besides this, social media users can also be vulnerable in a personal and not relational sense – e.g. due to their age or financial standing. This source of vulnerability, however, is rarely considered in separation from vulnerability that stems from forming a market or social relation in the online environment (see also Galli *supra* (fn. 5), at 194, 196).

78 See e.g. the practice of amplifying the user's extreme emotions in construing a newsfeed as acknowledged by Facebook – Goel, 'Facebook Tinkers With Users' Emotions in News Feed Experiment, Stirring Outcry', New York Times, 29 June 2014.

79 Ezpeleta / Zurutuza / Gómez Hidalgo, A study of the personalization of spam content using Facebook public information, 25 Logic Journal of the IGPL 30 (2017).

80 See e.g. Amilo, Speech Regulation by Algorithm, 30 Wm. & Mary Bill Rts. J. 245 (2021-2022).

to digital architecture and governance structures supplied by a non-state third party. In this way, consumers make themselves vulnerable to the manner in which platforms exercise their private governing power.[81] Referring one more time to the social media example, users seeking social relations and self-expression online subject themselves to content moderation, account suspension and other forms of platform governance that can harm their private sphere and personal interests. The similar susceptibility to arbitrary exercises of power by online platforms is also typical for the other digital economy domains that cater for user emotions and social experience (such as dating apps, discussion fora and online gaming platforms).

Further, the quality question usually involves strong consumer expectations regarding the safety of relationships built online, the security of data and protection from other users' deception and violence. These expectations are in themselves a source of consumer vulnerability. By entrusting their emotions and social liaisons to an online service provider, consumers put themselves in a precarious position, making important parts of their personal sphere dependent on a commercial market actor. Thus, the pivot of the system is users' reliance on the proper quality of speech infrastructure supplied to them. This trust relation overlaps with the personal consumer values discussed earlier as the first pillar of post-consumer digital vulnerability. Indeed, expectations as to informational safety and autonomy can be seen as a common denominator for the personality- and quality-related components of this concept.[82] This general framework applies to the fullest extent to social media platforms. It can, however, also incorporate the other types of digital services that centre around user experiences, emotions and social links. The sources of post-consumer digital vulnerability can be structured in the following way:

81 Tsesis, Dignity and Speech: The Regulation of Hate Speech in a Democracy, 44 Wake Forest Law Review 497 (2009).

82 See e.g. Custers / van der Hof / Schermer, Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, 6 Policy & Internet 268 (2014).

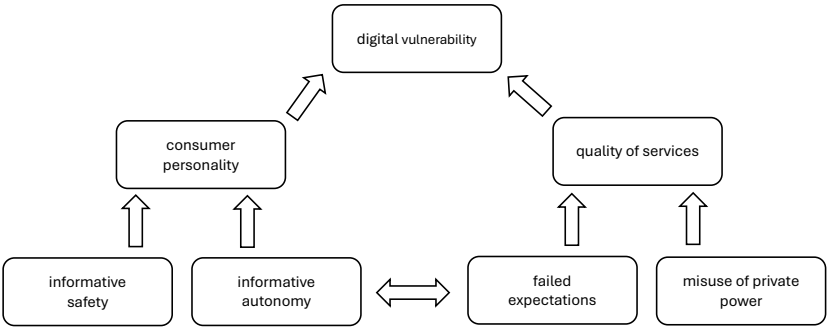


Fig. 2 – Digital vulnerability: the case of post-consumptive services

III. Digital vulnerability: towards a comprehensive concept

Post-consumer digital vulnerability responds to the need for a conceptual framework for consumer interests and consumer harm that goes beyond the conventional framework of consumer law. It aims to supplement the general concept of digital vulnerability – as a relational (situational) and architectural[83] consumer feature – with another dimension, typical for the consumption patterns increasingly prominent on the market. Thus, the concepts of general consumer vulnerability and of the post-consumer are complementary and can create a thorough conceptual understanding of the essence and peculiar sources of consumer weakness in the online realm.

The various origins and instances of the post-consumer vulnerability discussed in the previous section share three common features: (a) they incorporate non-economic consumer interests[84] addressed by online platforms; (b) they stem from the technical organization of consumer services combined with the power relationships on the market; (c) they are situation-based and do not relate to distinctive personal features such as age or wealth. It is easy to notice that the two modes of consumer digital vulnerability discussed in this section share the same conceptual grid. They

83 On the relational and architectural concept of digital vulnerability, see fn. 67.

84 Undeniably, the fact that the interests in question are of non-economic nature does not preclude contracts concluded with social media platforms and other service providers from being reciprocal. In most instances, such reciprocity is based on an exchange of consumer data for various infrastructures supplied by platforms (see also fn. 45).

both rest on the assumption that certain types of market activity expose individuals to a higher degree of risk, by amplifying existing market weaknesses or by triggering new ones. In this sense, every consumer – solely by being a human – bears in herself digital vulnerability that can be activated under the particular market conditions. Thus, both types of digital vulnerability are situation-based (relational) and dependent on the technological and private regulatory design of the particular consumer service. For this reason, the two senses of vulnerability shares many of their origins, such as the widespread use of algorithms in governing platform-user relationships, the severe imbalance of bargaining power, and the issue of protecting consumers' private sphere.

The difference between these two modes of vulnerability rests on differences in subject-matter – or, to put it differently, in the various consumption patterns that underpin them. The post-consumer realm pertains to activities that the classical legal imaginary would allocate to the sphere of personality or fundamental rights, rather than to market issues per se. With the ongoing commodification of these spheres in the digital market, problems expressed so far in the language of social autonomy, freedom of speech and analogous notions have to be reconceptualized as parts of a market regulation framework. To put it in different terms, the essence of 'post-consumer' digital vulnerability rests in the nature of the values involved. First, by seeking experiences, social interactions and emotions, consumers expose inherently sensitive parts of themselves to service providers. This includes, for instance, information about their personal life, health and other intimate details that are usually kept private or revealed only to one's close circles of family and friends. Second, the commodities catered for in the post-consumer domain are also sensitive in themselves, as they address the intimate, oftentimes fundamental, personal and social needs of human beings. For the reasons discussed in the previous section, the technological design of social infrastructures sifts the power/weakness relationship in the post-consumer realm and exposes consumers to even higher levels of potential harm. Consequently, similar to the modern concept of digital vulnerability, its post-consumer version can also be perceived as both relational and architectural. However, both the market/social situation and the technological design employed to govern users' interactions is located elsewhere.

For these reasons the quality of these services and their compliance with users' expectations relate to intrinsic features of human beings and

need to be conceptualized in terms other than the typical commodities encountered in the consumer economy. At the same time, however, since they are traded on the market and subjected to the overall economic logic, they must be embraced by a general formula of consumer interests and consumer harm. It is necessary not only for instrumental reasons (i.e. to ensure a consistent applications of tools such as the UCTD), but also for more political consistency across various parts of the EU digital law.[85] The concept of digital vulnerability put forward in this chapter attempts to identify the main types of consumer weakness in these sectors of the digital economy. Its concept is an organic ramification of the existing consumer law, and it builds on the already existing tendencies to incorporate interests and other types of market involvement that do not amount to conventional economically oriented consumption.

From this vantage point, post-consumer digital vulnerability aims not to directly subvert the concept of digital vulnerability, but rather to supplement the economic and social imaginary on which it was founded. EU consumer law is in acute need of a more integrative concept of weakness/vulnerability, which would take into account the divergence of commodities consumers seek on the market and which would reach beyond the classical set of value/price questions. The concept outlined in this paper allows an integration of these domains by setting parameters for understanding consumer interests that lie outside the classical core of consumer law. Hence, it is necessary to develop an integrative concept of consumer vulnerability that would encompass the broader heterogeneity of present-day consumption.

E. The way ahead: bridging consumer law and platform regulation

The thorough idea of consumer vulnerability is even more important from the perspective of recent developments in the regulation of online platforms in EU law. Current EU legislation tilts towards separating the protection of consumers and users of other services online. This pertains especially to the DSA but also to other acts, such as the recent Regulation on political

85 See also the next section.

advertising.[86] This split[87] is rather unnatural from the perspective of the matter involved, which encapsulates both protection of individual vis-à-vis a firm (i.e. a typical consumer law matter) and protection of members of society or the polity who engage themselves in interactions intermediated by online platforms.[88] Consequently, platform regulation overlaps not only with the subject-matter of consumer law[89] but also with several instruments designed primarily to protect consumers.[90]

EU law does not seem to build many bridges across these instruments. In its current state, it leaves out several issues regarding the coordination of rights and enforcement schemes. These gaps may be filed by general consumer law instruments (such as the UCTD and UCPD). This requires, however, a coherent understanding of why consumer protection in the platform economy differs from more conventional settings, and an understanding of what the object of this protection should be. The examples from case law discussed earlier[91] illustrate well the struggle between older forms of consumer protection (UCTD) and the need to conceptualize new forms of consumer harm that do not fit into the conventional imaginary of consumer law. The resort to fundamental rights as a benchmark in conceptualizing consumer interests and vulnerability, although convincing as an interim solution, clearly does not provide a satisfactory answer to

86 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, OJ L, 2024/900, 20.3.2024.

87 See, especially, recital 10 DSA, stating that "for reasons of clarity, this Regulation should be without prejudice to Union law on consumer protection, in particular Regulations (EU) 2017/2394 and (EU) 2019/1020 of the European Parliament and of the Council, Directives 2001/95/EC, 2005/29/EC, 2011/83/EU and 2013/11/EU of the European Parliament and of the Council, and Council Directive 93/13/EEC, and on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council."

88 The perception of user vulnerability in the DSA builds on a personal rather than a relational view (see recitals 62, 95 and 104, which mention minors as the illustrative instance of vulnerable recipients of online services).

89 See Busch / Mak, Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation, 10 *Journal of European Consumer and Market Law* 109 (2021); Caufman / Goanta, A New Order: The Digital Services Act and Consumer Protection, 12 European Journal of Risk Regulation 758 (2021).

90 See e.g. Article 14 DSA, which introduces substantive requirements for terms of service, and Articles 25–27 DSA on online transparency and counteracting manipulation.

91 See section C.II.

the structural question of protecting consumers who opt for non-economic consumption modes.

The broader concept of digital vulnerability allows for a remedying of this weakness, by accommodate new modes of consumer interest as a part of a coherent consumer law framework. It offers a better understanding of the extent to which certain platform services can be classified as consumer commodities that can be put under the same rubric as other commodities on the consumer market. In this way, it can create a common denominator for cross-references between platform and consumer rules, in particular for a reciprocal formulation of the values and concepts developed in these spheres.[92]

Finally, the augmented formula of consumer vulnerability puts into broader context the use of fundamental rights, which play a crucial role within the DSA, and – as was earlier demonstrated – which gain prominence in the treatment of consumer law issues.[93] From this perspective, the recourse to fundamental rights can be seen in a twofold way. First, it serves an indicative function by clearly pointing out that certain spheres of platform/user relationships are particularly sensitive for the legal order – and, hence, that they may trigger especially high degrees of vulnerability. Thus, fundamental rights provide an overall mapping of issues that necessitate attention in setting and enforcing rules for the digital economy.

Second, at a more granular level, fundamental rights may indeed serve as quality benchmarks for online services. The speech-related case law discussed earlier marks some origins of this trend, and the vividly constitutional perspective of the DSA is likely to further amplify it. In having recourse to fundamental rights as a yardstick for consumer services, one caveat is needed. Undoubtedly, while fundamental rights (such as freedom of speech) may provide a point of reference in deciding whether a particular platform service respects basic user rights, they do not exhaust the entire spectrum of consumer vulnerability. Rather, it encompasses a broad range

92 Interestingly, the DSA also seems to implicitly subscribe to a more diversified concept of user interest and harm, one which combines economic and non-economic substrates. See, for instance, recital 69 of its preamble, which identifies the following problem with online advertising addressed to vulnerable users: 'When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups.'

93 See the case law discussed above in section C.II.

of interests that cannot be reduced to purely constitutional dilemmas and a balancing of fundamental rights. The comprehensive concept of consumer vulnerability discussed in this chapter speaks in favour of adopting a different perspective, one where the interests of individuals participating in the digital economy are seen as falling along a continuum. It puts economic and non-economic values on the same footing and treats them as self-sufficient parameters of a properly functioning digital consumer economy.

Digital Vulnerability as a Power Relation: Hyper- and Hypo-Autonomy and Why Thick Privacy Matters

Irina Domurath

A. Introduction

Vulnerability has been a topic in EU Law at least since the adoption of the Unfair Commercial Practices Directive (EC) 2005/29 (hereinafter UCPD).[1] The point that is repeatedly being made is that there are different risk factors that can lead to consumer vulnerability in certain fields.[2] There is widespread agreement among EU consumer law scholars that the protective standard of the reasonably circumspect consumer in EU Law is a normative standard that has not much to do with reality and, more importantly, does not adequately protect European consumers. Nevertheless, the reasonably-circumspect-consumer standard has remained in place. Nowadays, there is a renewed interest in the concept of vulnerability, converging again to a remarkable agreement in EU consumer law scholarship that digital technologies have led to new vulnerabilities of consumers.[3] The very premise of this volume is that digital technologies create a new type of vulnerability: digital vulnerability.

1 Directive 2005/29/EC of the European Parliament and of the Council 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').

2 For example, Peter Cartwright, 'Understanding and Protecting Vulnerable Financial Consumers' [2015] Journal of Consumer Policy; Norbert Reich, 'Vulnerable Consumers in EU Law' in Dorota Lecykiewicz and Stephen Weatherill (eds), *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law* (Hart Publishing 2016); Jan Trzaskowski, 'Is It Unfair to Mislead Vulnerable Consumers ?' 1, Irina Domurath, *Consumer Vulnerability and Welfare in Mortgage Contracts* (Hart Publishing 2017).

3 See for example Christine Riefa, *Protecting Vulnerable Consumers in the Digital Single Market*, 33 Eur. Bus. Law Rev. 607–634 (2022).

What has aided this scholarly agreement on 'digital vulnerability' is the ubiquity and opacity of data collection embedded in an almost casual (hardly debated) surveillance context. Surveillance - not in the traditional sense by states and public authorities - but also and especially by private companies whose very business models lies on the collection, analysis, and sale of consumer data has become extremely pervasive.[4] The political economy terms for this are 'surveillance capitalism' and 'informational capitalism'. The first refers to a new form of capitalism that aims to predict and modify human behaviour as a means to produce revenue and gain market control.[5] 'Information capitalism' describes the alignment of capitalism as a mode of production with informationalism (accumulation of knowledge and higher levels of complexity in information processing) as a mode of development,[6] where market actors use knowledge, culture, and networked information technologies in order to extract and appropriate surplus value.[7] This surplus value is created through personalized marketing algorithms, which are specifically designed to exploit consumer weaknesses. These systematic influences at the precise time an individual is irrational collapse any meaningful distinction between the rational, normatively average and vulnerable consumer.[8] They undermine any idea of standardized protection, including the taking-into-account of collateral damage for non-average-consumers.[9] In times of personalised marketing, the idea of an 'average' consumer is outdated.

Surveillance is made possible by large-scale privacy intrusions. New technologies have not only increased the extent of what is being monitored is (more permanent data) but have also made searching more efficient and cheaper, which increases the burden of monitoring; the limits of privacy

4 Frank Pasquale, Black Box Society - The Secret Algorithms that Control Money and Information (2015).

5 Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75.

6 Manuel Castells, *The Information Age Vol I: The Rise of the Network Society* (Blackwell Publishing 1996), 14–18.

7 Julie E Cohen, *Between Truth and Power - The Legal Constructions of Informational Capitalism* (Oxford University Press 2019), 5-6.

8 Ryan Calo, *Digital market manipulation*, 82 George Washington Law Rev. 995–1051 (2014), 1033.

9 Jan Trzaskowski, Your Privacy Is Important To Us! - Restoring Human Dignity in Data-Driven Marketing (2022).

are eroded.[10] In fact, data protection regimes are reflections of the idea that all individuals are 'vulnerable' to power balances created by digital technologies.[11]

Privacy is however neglected in the current conceptualizations of *digital vulnerability*. While discussions on the digital vulnerability of consumers have already brought about a thickened understanding of what digital vulnerability is and where it comes from, the concept of privacy is still a neglected and under-conceptualized component of the concept. This contribution aims to remedy this neglect and analyse the role of privacy – and also what type of privacy – for the concept of digital vulnerability. It brings together the discussions surrounding digital vulnerability and privacy with a view to connecting the two concepts. In this way, the hope is to enable further discussions in order to understand the impact of a lack of privacy on digital vulnerability.

In what follows, I will first outline the discussions on vulnerability in EU Law (B), including criticism to the way in which vulnerability is hitherto understood and the proposals for adopting the concept of digital vulnerability. I will characterize *digital vulnerability* as a power relation, in which the hypo-autonomy of consumers contrasts with the hyper-autonomy of structurally powerful companies. Then, I will turn to the idea of privacy (C), explain its intrinsic value, before contrasting the what I call thin understanding of privacy in EU Law with a thick understanding of privacy in the privacy literature. Finally, I will explain how the concept of digital vulnerability can benefit from incorporating a thick concept of privacy (D).

B. Vulnerability in EU Law

In this section, I will distinguish the concept of (general) vulnerability and the new concept of digital vulnerability. While the first is well-known in EU Law, the second is not yet part of the EU legal order even though pushes towards broader interpretations of the framework exist.

10 Lawrence Lessig, *The Architecture of Privacy: Remaking Privacy in Cyberspace*, 1 Vanderbilt J. Entertain. Technol. Law 56–65 (1999).

11 Calo, *supra* note 8.

I. Static, personal, exceptional

The concept of vulnerability is well known in EU consumer law. It describes a category of consumers, who are – according to Article 5 (3) UCPD - 'particularly vulnerable' to certain commercial practices 'because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee.' The concept of vulnerability serves to assess the (un)fairness of the commercial practice in question from the perspective of the average member of that vulnerable group. It does not lead to higher standards of information or more obligations of traders. Instead, it serves as a factor when assessing the unfairness of a commercial practices. Vulnerable consumers are the ones who are at a higher risk of experiencing negative outcomes in the market, have limited ability to maximise their well-being, have difficulty in accessing information, are less able to choose and buy, or are more susceptible to certain marketing practices.[12]

Otherwise, consumer law does not contain many references to vulnerability. For the digital sphere, the DSA works with a similar concept of vulnerability with regard to countering illegal hate speech on platforms. Recitals 62, 95, and 104 DSA mention 'vulnerable recipients of the service, such as minors.' Recital 94 DSA stipulates that assessments and mitigations of risk with regard to recommender systems need to elicit measures to 'prevent or minimise biases that lead to the discrimination of persons in vulnerable situations, in particular where such adjustment is in accordance with data protection law and when the information is personalised on the basis of special categories of personal data' of Article 9 GDPR.

In European technology and data law, the approach is very similar. Art 5 I lit b) AI Act prohibits AI systems that exploit the 'vulnerabilities of a specific group of persons due to their age, physical or mental disability'. Similarly to Art 5 (3) UCPD, it emphasizes the goal of materially distorting' the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm.' Notably, Article 5 I AI Act moves away from using 'vulnerability' as a means to *assess* fairness to using it as a constituting element for a prohibition of technology. In the GDPR, the only mention of vulnerability

12 European Commission, Study on consumer vulnerability in key markets across the European Union (EACH/2013/CP/08), http://ec. europa.eu/consumers/consumer_evidence/market_studies/vulnerability/index_en.htm.

can be found in Recital 75, which refers to the 'personal data of vulnerable persons, in particular of children' as a category of data the processing of which poses a risk to the rights and freedoms of natural persons. According to Recital 38 GDPR, specific protection should apply where personal data of children is used for the purposes of marketing or profiling. In terms of legal consequences, only information-related rules can be found in the GDPR, see for example Article 40 II lit g) GDPR.

A few aspects stand out in these uses of *vulnerability*. It is regarded as an exception to the rule of non-vulnerable people. In consumer law, the reasonably circumspect consumer is the normative benchmark, whereas vulnerability is circumscribed to a special type of person. It refers to a specific group of people that is in need of special protection, arguably as opposed to other 'normal' people. What is more, the concept of vulnerability is a personal one. It is based on personal status or characteristics, usually relating to impaired cognitive capacity. Children and the elderly are considered vulnerable because their age is connected to cognitive limitations. Mental disability is another personal characteristic that is considered to lead to cognitive limitations. These limitations are the reason for applying more protective rules. *Vulnerability* is also a static concept: autonomy-impairment is considered to underlie all dealings of those individuals, which is the precise reason why there are afforded special and exceptional protection. This also holds true for the more general prohibitions in the AI Act. For those reasons, the static and personalistic approach to vulnerability in EU Law has been subject to criticism and ample discussion.[13]

13 Geraint G Howells, HW Micklitz and Thomas Wilhelmsson, *European Fair Trading Law - The Unfair Commercial Practices Directive* (Ashgate 2006), 111-117. This dichotomy has been criticized in the literature, for example in Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking EU Consumer Law* (Routledge 2018); but especially so in the field of financial services, see for example: Peter Cartwright, 'The Vulnerable Consumer of Financial Services: Law, Policy and Regulation' 1; Peter Cartwright, 'Understanding and Protecting Vulnerable Financial Consumers' [2015] Journal of Consumer Policy; Lorna Fox O'Mahony, Christian Twigg-Flesner and Folarin Akinbami, 'Conceptualizing the Consumer of Financial Services: A New Approach?' (2015) 38 Journal of Consumer Policy 111; Irina Domurath, *Consumer Vulnerability and Welfare in Mortgage Contracts* (Hart Publishing 2017); Irina Domurath, 'The Case for Vulnerability as the Normative Standard in European Consumer Credit and Mortgage Law – An Inquiry into the Paradigms of Consumer Law' (2013) 3 Journal of European Consumer and Market Law 124.

In other words: consumer vulnerability is the impaired capacity to act on the market in accordance with one's self-interest.[14] It finds its basis in the idea of impaired autonomy. While the reasonably circumspect, fully autonomous consumer in EU Law benefits from freedom of contract and negotiation or unfairness control of contracts of adhesion, the less autonomous ones are protected (in specific) instances.[15] Article 5 (3) UCPD concerning the danger of manipulation and Art 5 (1) lit b) Proposed AI Act are examples of this approach. Autonomy is understood as freedom from manipulation. In the UCPD, the reference point is young age, physical or mental disability, or incredulity, as examples of diminished autonomy, which make the people concerned vulnerable to the distortion of their economic behaviour. Because of young age or some other personal impairment, there is an increased risk of entering into agreements that distort their behaviour. In any case, impaired personal autonomy leads to vulnerability, namely the subjection to manipulation of economic behaviour.

II. Digital vulnerability

Consumer research argues that the reasonable circumspect consumer as a standard for protection under EU Law is obsolete in the digital sphere because digital vulnerability affects everyone. It is universal. This reverses the current vulnerable-not vulnerable dichotomy.[16] Consequentially, proponents of the adoption of a *digital vulnerability* concept argue for a regulatory shift and the reversal of the current vulnerability-paradigm, especially in unfair commercial practices law. Instead of seeing the vulnerable consumer as an exception to the normative benchmark of the reasonably circumspect consumer, they acknowledge that all consumers are – albeit in different degrees – vulnerable to exploitative practices. This goes beyond the proposal of the EU Commission to modulate the average-consumer-test in the digital sphere, even to the perspective of one single person, if the

14 Calo, *supra* note 98, 1034.

15 Howells, Twigg-Flesner, and Wilhelmsson, *supra* note 13, 27 et sub.

16 Natali Helberger et al., *EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets*, EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets - A joint report from research conducted under the EUCP2.0 project (2021), at 5; Federico Galli, Algorithmic Marketing and EU Law on Unfair Commercial Practices (2022), 205.

practice is highly personalized.[17] With this approach, the Commission does not give the average-vulnerable dichotomy, but merely tweaks the vulnerability-assessment.

Research on digital vulnerability draws on the concept of intersectionality,[18] attempting at a more multi-faceted and less static idea of vulnerability. Definitions of digital vulnerability now converge towards an understanding that emphasizes structural asymmetries in the *relation* between actors rather than personal characteristics of *individuals*. Two characteristics of the concept distinguish it from the current static and personalistic understanding of vulnerability in EU Law: it is relational and layered.

1. Influence of intersectionality: vulnerability as relational

The probably most influential contemporary conceptualizations of vulnerability are the ones by feminist scholars Fineman and Luna. According to Fineman, vulnerability derives from our embodied humanity that carries with it the ever-present possibility of harm.[19] Because of different economic and institutional positions and relationships, individual vulnerability occurs at a range in magnitude and potential. Fineman's universal, human vulnerability is experienced uniquely by each individual and is greatly influenced by the quality and quantity of the resources we possess or can command.[20] Luna conceptualizes Fineman's idea of the individual experiences of an inherently human vulnerability with an intersectional perspective.[21] She argues that vulnerability is layered and relational.[22] She observes that depending on the specific circumstances – whether political, economic, social, cultural - people can acquire layers of vulnerability. Vulnerability is relational, because people are not vulnerable per se, but are

17 EU 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 (2021/C 526/01), 100.

18 The concept was introduced by Kimberle Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 Fem. Leg. Theor. 139–167 (1989).

19 Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20 Yale Journal of Law and Feminism 1, 9.

20 ibid., 10.

21 Crenshaw, *supra* note 18.

22 Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 International Journal of Feminist Approaches to Bioethics 121, 128-129.

rather *made* vulnerable. Varied and changing circumstances render individuals vulnerable.[23] Everybody can be vulnerable in certain circumstances and the circumstances do not necessarily occur naturally but can also be engineered and controlled. Vulnerability conceptualized as a layered and relational universal human experience has moved the discussions beyond binary dichotomies where vulnerability is or is not situated in static, personal characteristics leading to stigmatization and discrimination.

2. Two definitions

Helberger et al put forward a concept of digital vulnerability that is based on a refined, universalist idea of Fineman that vulnerability is an ever-present possibility of harm or misfortune. Fine-tuning the concept to the digital age, they define digital vulnerability as a universal state of defencelessness and susceptibility to power imbalances' in the digital sphere, characterized by automation of commerce, datafied consumer-seller relationships and the architecture of the digital marketplace.[24] They argue that digital vulnerability needs to be a dynamic concept that responds to the adaptive persuasive systems employed in digital marketing.[25] Following Rogers et al,[26] they distinguish between inherent (Fineman's) and situational sources of vulnerability on the one hand, and dispositional (potential) and occurrent (manifest) states of vulnerability.[27] Fitting also with, however not specifically referring to, Luna's conceptualization, they emphasize that digital vulnerability is both architectural, meaning the – not accidental - product of digital consumer markets as well as relational - manifest in the ongoing asymmetrical relation between consumers and service providers.

Galli, in turn, adopts more specifically Luna's idea of layers. For him, digital vulnerability – understood as a potential negative impact on consumer wellbeing in the digital sphere -[28] in the context of algorithmic marketing consists of four layers, which can interact, albeit not necessarily. The foundational layer of all digital vulnerability, for Galli, is the architecture, the 'objective way of being', of algorithmic marketing that makes

23 ibid.
24 Helberger et al., *supra* note 16, 5.
25 Helberger et al., *supra* note 16, at 183.
26 Wendy Rogers, Catriona MacKenzie & Susan Dodds, *Why bioethics needs a concept of vulnerability*, 5 Int. J. Fem. Approaches Bioeth. 11–38 (2012).
27 Helberger et al., *supra* note 16, 184-185.
28 Galli, *supra* note 16, 192.

everybody vulnerable who is active on the digital market. The second layer consists of privacy as the increasing function of autonomy vis-à-vis sellers. Third, situational vulnerabilities can exist that relate to personal and consumption-relation situations and patterns, such as consumption intervals or behavioural limitations in decision-making. The upper layer consists of personal characteristics, such as age or mental conditions. In this conceptualization, the architectural layer that concerns all consumers is the one that always remains, even if the other layers are not present in any given case.

Both accounts understand vulnerability as a more dynamic and universal situation than is acknowledged in current EU Law. They put emphasis on the architectural nature of vulnerability: Helberger et al stress that vulnerability is the necessary, and even intentional, product of the choice-architecture on digital consumer markets,[29] while Galli highlights that the way in which algorithmic marketing is made (architecture) 'cascades through' all other layers of vulnerability.[30]

3. Hyper- and hypo-autonomy: the power relation in digital vulnerability

The two ideas of digital vulnerability fit well with a definition of vulnerability I proposed elsewhere: the exposure to risk and the lack of resilience to avoid harm from the materialization of those risks.[31] Updated for the digital sphere, the exposure to risks come from the design of commercial practices on digital markets (what Helberger et al and Galli call 'architecture'), whereas the lack of resilience describes the lack of power of consumers vis-à-vis transnational companies. This relation can be understood as a relation of power in which the actors have different degrees of autonomy: companies have increased (hyper-)autonomy, whereas the consumers have decreased (hypo-)autonomy. Understanding vulnerability as a power relation, highlights the shortcomings of the EU Law approach which focuses solely on the hypo-autonomy of the consumer side, while neglecting the hyper-autonomy of companies.

29 Helberger et al., *supra* note 16, 187; also Galli, *supra* note 16, 203.
30 Galli, ibid, 204.
31 Put forward for financial services, see Domurath, *supra* note 2, 64.

a) Autonomy

While definitions of autonomy are numerous – oscillating in between liberty, self-rule, or free will,[32] I consider it useful to use Christman's conceptual distinction between individualistic and relational understandings of autonomy.[33] Both are concerned with the conditions for some kind of authenticity of will and action. I understand the discussions to be concerned with the conditions in which self-determination and authenticity can come about. Some authors put emphasis on the governance in one's actions and life by values, principles, or reflections that are truly their own as opposed to being guided by external or even manipulative forces.[34] Authenticity refers to a 'wholeheartedness' or 'truthfulness' connected to free will. It 'concerns the independence and authenticity of the desires (values, emotions, etc.) that move one to act in the first place.'[35] In this view, autonomy describes the possibility of being directed by considerations, desires, conditions, and characteristics that are not externally imposed, but which are part of one's authentic self.[36] The individualist approach emphasizes self-rule, authenticity (genuineness of values), and competence to relational thought. This does not necessarily mean that individuals need to be able to reflect on their subjective values in complete isolation from cultural and social context. In fact, Kymlicka argues that it is enough for a liberal notion of autonomy, 'piecemeal reflection' to enable individuals to engage critically with value formation.[37]

32 See for an exemplary overview of definitions, Gerald Dworkin, *The Theory and Practice of Autonomy* (Cambridge University Press 1988), 5; also: Andrew Sneddon, autonomy (Bloomsbury Academic, 2013), 2 ff.

33 John Christman, *Autonomy in Moral and Political Philosophy*, The Stanford Encyclopedia of Philosophy (2020), https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/.

34 John Christman, *Autonomy*, *in* The Oxford Handbook of the History of Ethics 691–709 (2013).

35 ibid. To what extent authenticity is required for autonomy, is highly debated. See, negatively: Sneddon, *supra* note 31, 7.

36 Christman, *supra* note 34. This view needs to be distinguished from moral philosophical viewpoints dealing with the responsibilities and obligations flowing from autonomy.

37 He does so within his argument that group rights are not logically opposed or in detriment to individual autonomy, see: Will Kymlicka, Multicultural Citizenship (1995).

Relational or social views on autonomy emphasize the specific environment in which self-governing agents find themselves. It is argued that the self has basic values which are filtered through social relationships. For example, in feminist studies, Mackenzie and Stoljar argue that personal and social relationships have constituent power over the development of people's identities and that the alienation following detachment from those relationships would undermine autonomy.[38] Thus, they shed light on the social conditions that can further or limits the ability to act effectively upon one's own values, emphasizing that the creation and exercise of autonomy is shaped by interpersonal relations and interactions. Social practices thus become constitutive elements of autonomy.[39] There is also a view that Christman calls 'procedural', which demands to look at the procedures by which individuals come to identify their values as their own in order to determine authenticity of value. This view is concerned with guaranteeing neutrality towards all conceptions of value.[40]

The way I see it, the disagreement between those views consists in the degrees of detachment from as well as the definition of 'external factors' for the constitution of autonomy. While the more individualistic view seems to operate on a rather sharp distinction between what is internal and external, the more relational or social view accepts that internal and external factors for autonomy cannot be neatly separated and that the boundaries between the two are porous. What they have in common is a shared concern for the conditions in which personal (maybe even authentic) values can emerge, flourish, and be owned. The conditions for the capacity for self-rule are the main concern, with debates surrounding the issue of to what extent self-rule can be socially mediated.

b) Hypo-autonomy: lack of power of consumers

This puts emphasis on the question of whether and to what extent the conditions for self-rule and determination actually exist in the digital sphere,

38 C Mackenzie and N (eds) Stoljar, *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (Oxford University Press 2000).

39 For an overview of the discussions, see Christman, *supra* note 34.

40 Dworkin does not use the concept of autonomy, but it is clearly underlying his idea of liberalism as concerned with equality, see Ronald Dworkin, 'Liberalism' in Stuart Hampshire (ed), *Public and Private Morality* (Cambridge University Press 1978), 115.

namely to what extent consumers are actually autonomous. Different issues should be conceptually distinguished here.

We know that all consumers are considered to be in an inferior bargaining position due to information asymmetries and standard term contracts.[41] These are the very reasons for the regulation of consumer markets in the first place. Here, consumer autonomy is supposed to be intact, because the consumers have had time to reflect upon their values and choices as consumers, but the external condition of non-negotiable terms impede them to act in accordance with those choices. As a consequence, consumers are stuck with contracts terms that they did not choose. The regulatory approach here is to allow for the control of unfairness,[42] in order to ensure that the consumer who is left with no choice is at least not left with an obligation to adhere to unfair terms. Consumer autonomy is established ex post.[43]

There are however behavioural issues, which impede rational consumer decision-making, thereby leading to market failures.[44] There is a normative relation between autonomy and rationality. At times, consumer autonomy can be intact, but external conditions impede individuals from acting rationally in conformity with their self-determination and autonomously formed will. For example, consumers might not be able to deal with situations of pressure such as doorstep selling and, as a consequence, end up buying products and services that they did not want in the first place. Again, EU Law steps in.[45] Similarly, people affected by a serious illness could be considered vulnerable to particular advertising that misleadingly

41 Friedrich Kessler, *Contracts of Adhesion - Some Thoughts About Freedom of Contract*, Columbia Law Rev. 629–642 (1943).

42 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, 29–34.

43 See doctoral thesis of Candida Leone, on file with author.

44 See the 2011 Special Issue in the Journal of Consumer Policy as well as the introduction thereto: Hans-W. Micklitz, Lucia A Reisch & Kornelia Hagen, *An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law,"* 34 J. Consum. Policy 271 (2011), http://proquest.umi.com/pqdlink?did=2436552091&Fmt=7&clientId=58117&RQT=309&VName=PQD.

45 Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises, OJ L 372, 31.12.1985, 31–33.

presents products as able to cure their illness,[46] precisely because – even though their autonomy is intact (including the wish to be cured), they are susceptible to a certain type of marketing that exploits their wish to be cured. This is precisely the approach of Article 5 (3) UCPD. In other instances, consumers do not always act rationally due to cognitive limitations. Here, autonomy could be considered impaired because preferences might be sup-optimal. This is the behavioural economics critique, which has, however not yet led to a change of regulatory approach.

In contrast, the concept of exceptional consumer vulnerability as currently included in the EU Law framework presupposes that vulnerable consumers are not autonomous due to their specific, personal characteristics such as age or mental infirmity. Those consumers are inhibited in their self-determination, because they are not able to develop autonomous will. For example, most legal orders restrict legal competence of minors. In addition, the UCPD, prohibits as unfair practices that exploit limited autonomy. The EU considered teenagers immature and credulous, which is why they can succumb to rogue marketing practices due to their lack of attention or reflection or risk-taking behaviour.[47] Therefore, the EU puts in place special protection measures in order to ensure that these consumers are protected from any possible negative consequences.

In the digital sphere, the autonomy of consumers is even more diminished: it is hypo-autonomy. This hypo-autonomy derives from the combination of mainly two issues: big data and the long-term character of consumer-business relations in the digital sphere. First, the increasing generation and accumulation of ever more data enables consumer data, combined with the use of algorithms and AI, into information usable for commercial purposes. The collected data can give insights into 'socio-demographic characteristics, such as age, gender or financial situation, as well as personal or psychological characteristics, such as interests, preferences, psychological profile and mood. This enables traders to learn more about consumers,

46 For example in an Italian case concerning 'slimming pills', see Autorità Garante della Concorrenza e del Mercato, Provvedimento n. 24607, PS6980 – *Xenalis Dimagranti*, ll.

47 European Commission, 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, (2021/C 526/01), 36.

including about their vulnerabilities.'[48] With the possibility to infer increasingly fine-grained (and maybe even correct) consumer profiles from more and more collected data also come more possibilities to sell advertisements and products that are particularly tailored to exploit consumer biases and other vulnerabilities. Second, consumers' ongoing involvement in digital products and services make them increasingly susceptible to manipulation: the longer the relationship between a consumer and a digital service or app persists, the more the app or service establishes a position of power as a result of increased knowledge about its users'.[49] The more companies know about their customers, the more 'insidious' and subconscious their attempts of influence can become.

This is where the concept of digital vulnerability comes in. *Digital vulnerability* is more than just a situation or an 'unfortunate by-product' of economic activity in the digital sphere, but deliberately created,[50] sustained, and exploited for financial gain. It lies at the heart of capitalist logic that the systematically irrational behaviour of individuals will be exploited.[51] Engaging in 'nudging for profit' is following the economic incentive.[52] It is the very design of personalized products to respond to individual vulnerabilities. Nudging and discrimination as part of manipulation and exploitation are, thus, the problems most criticized in consumer research.[53] The critique puts emphasis on the effects of the 'industry's relentless search for experimental and creative digital marketing practices that seek to influence

48 European Commission, 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, (2021/C 526/01), 36

49 Helberger et al., *supra* note 16, at 22. I do not agree, howevere, with Helbereger et al's claim that people move in and out of states of vulnerability. Especially with regard to algorithmic profiling, I think that the structuredness of the power relation with the company is so pervasive that 'digital vulnerability' is omnipresent and unflexible; or, at least, iindividuals move into stages of vulnerability more often than they move out of them.

50 Helberger and others (n 16), 19.

51 Jon D Hanson & Douglas A Kysar, *Taking Behavioralism Seriously: Some Problems of Market Manipulation*, 74 NYU Law Rev. 630–749 (1999), 635.

52 Calo, *supra* note 8,1001.

53 Philipp Hacker, 'Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law' [2021] European Law Journal 1; Calo, *supra* note 8; Tal Z Zarsky, 'Privacy and Manipulation in the Digital Age' (2019) 20 Theoretical Inquiries in Law 157; Karen Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design' (2017) 20 Information Communication and Society 118.

consumer behaviour'.[54] In this way, *digital vulnerability* also makes it clear that the hypo-autonomy of individuals is matched by increased autonomy of companies that create and exploit hypo-autonomy of individuals.

c) Hyper-autonomy: structural power of companies

The architectural aspect of vulnerability relates to the design of markets that brings about consumer vulnerability. In Helberger et al.'s view, the architectural character describes the fact that vulnerability is the very product of digital consumer markets; this relates to a type of 'situational monopoly' deriving from reduced choice for consumers, unequal bargaining power, and including the power of electronic devices.[55] For Galli, the architectural *layer* of vulnerability is based on four features:[56] horizontal and aggregate effects of data collection that enable access to individual consumers beyond individual data collection;[57] customization based on statistical (not necessarily truthful) prediction; usage over time, and the power concentration on digital markets. Both understandings of vulnerability thus stress that the way in which digital markets are *designed to* work by the very companies that trade and sell on those markets is leading to a universal vulnerability. Whether this is new or whether the digital sphere has only accentuated or shed light on existing consumer vulnerabilities on other markets[58] is not relevant here. What matters is that the way digital markets are made to work has given rise to acknowledging a *structural* aspect of vulnerability, namely the way in which companies generate and maintain structural asymmetries vis-à-vis their customers.

Here, the concept of digital vulnerability reflects the idea of structural power as established in Political Economy. According to Strange's seminal

54 Helberger et al., *supra* note 16, 15.
55 Helberger et al., *supra* note 16, 187.
56 Galli, *supra* note 16, 201 ff.
57 In this vein also: Salomé Viljoen, *A Relational Theory of Data Governance*, Yale Law Journal, 573–654 (2020).
58 See, for example, arguments in favour of a more universal concept of vulnerability of consumer son financial markets: Peter Cartwright, *supra* note 3; David Capper, *Protection of the Vulnerable in Financial Transactions – What the Common Law Vitiating Factors Can Do For You*, *in* Unconscionability in European Private Financial Transations - Protecting the Vulnerable 166–183 (Mel Kenny, James Devenney, & Lorna Fox O Mahony eds., 2010); Domurath, *supra* note 3.

definition, structural power describes the capacity of actors to shape and determine the structure of the global political economy within with states, their political institutions, economic enterprises, and professionals have to operate.[59] In the consumer realm, consumer manipulation is now the characterizing feature of consumer markets as market outcomes are determined by the ability of companies to control information, present choices and shape the setting in which market transactions occur.[60] Structural power is more than the power to decide how things are to be done. It includes the power to shape the frameworks within which all economic actors - states, individuals, corporate enterprises - relate to each other and among each other.

For the digital sphere, structural power describes the ability of companies to control data and information flows, present choices and shape the very setting for digital market transactions. Digital platforms are points of entry for the creation of new forms of private power in surveillance,[61] shaping the conditions of market entry, the scope for disruption and contestation, as well as the sources and manifestations of economic power, thereby replacing and rematerializing markets, all according to their own agendas and private interests of business expansion based on the commodification of data.[62] Kapczynski describes this as the monopoly power over information and markets, creating winner-takes-it-all dynamics and price discrimination through tailored offers and contract terms.[63] This structural power is relational because it increases or diminishes if one party also determined the surrounding structure of the relationship.[64] The more power digital companies have the more the power of consumers to have influence on their relation with that company diminishes.

What emerges is a picture of companies as hyper-autonomous actors not only in terms of their actions as architects of a highly exploitative and

59 Susan Strange, *States and Markets* (Bloomsbury Academic 2015/1988), 27.

60 Foreseen 20 years ago by Hanson and Kysar, *supra* note 51, 635.

61 Julie E Cohen, *Between Truth and Power - The Legal Constructions of Informational Capitalism* (Oxford University Press 2019), 235. She relies largely on Castell's seminal definition and conceptualization of 'informational capitalism', see Manuel Castells, *Rise of the Network Society* (Wiley-Blackwell 2010), 17-18.

62 ibid., 42.

63 Amy Kapczynski, 'The Law of Informational Capitalism The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power Between Truth and Power: The Legal Constructions of Informational Capitalism', Yale Law Journal, 1460 (2020).

64 Strange, *supra* note 59, 27.

opaque digital environment but also as regards the capacity to build this basically ubiquitous architecture in a more or less unrestrictive way. Consumers are unable to meet this power, being hypo-autonomous themselves. There is no global legal framework that forces these 'architectural companies' to take into account any external (outside of company business strategy) constraints. Business secrets, including algorithms, are fiercely protected under national, international, and EU Law. In this way, companies are not just autonomous in the sense of being to operate their business as they seem fit: beyond this, they also make the markets on which they act.

III. Interim conclusion 1

The conceptualizations of *digital vulnerability* emphasize a new phenomenon on consumer markets. The emergence of new marketing techniques based on large-scale data collection.

These techniques do not only exploit existing vulnerabilities but also *make* consumers vulnerable. I argue that this can be adequately understood as a power relation, in which the structural power of companies to make agreements with consumers but also create and design the very markets for those agreements is a sort of hyper-autonomy that is not matched by the hypo-autonomy of consumers, expressed as a defenceless vis-à-vis those practices.

Digital vulnerability puts our attention on the structural aspects of vulnerability in the digital sphere, thus enabling policies that focus on the supply side of digital consumer markets. This is an important policy agenda. However, as is, the concept of digital vulnerability does not go beyond the current emphasis on the protection of consumers from the negative consequences of their distorted economic behaviour. It is assumed that because of personalization that specifically targets vulnerabilities, consumers make economic decisions that they may come to regret afterwards. The regulatory focus is, thus, on the distorted expression of an otherwise intact personal will, which could emerge in a self-determined context but is changed to fit goals of economic gains at the moment the consumer enters into an economic relation with a provider of some digital product or service. It is protection ex post, after the formation of will and choice (however irrational it may be).

C. Privacy

I want to put forward for consideration that the concept of digital vulnerability could be stronger if it were to conceptualize the idea of privacy as the very foundation for any human action (including consumer choice).

To be sure, privacy does play a role in *digital vulnerability*. Helberger et al mention that a lack of privacy can be a potential source of vulnerability and that the GDPR suffers from a similar outdated approach as the UCPD; the former distinguishes between 'sensitive data' and non-sensitive data in a similar way as the latter distinguishes between vulnerable and non-vulnerable consumers.[65] And Galli sees privacy as the second layer of vulnerability.[66] Both accounts see privacy as an autonomy-enhancing value.[67] And both accounts see privacy as a possible source of vulnerability. Calo, in turn, formulated the relation between privacy and vulnerability in this way: the more vulnerability there is, the less privacy there is, and vice versa. In the latter sense, privacy acts as a shield that places barriers in the way of discovering vulnerability.[68] Here, the function of privacy is to minimize exploitation by hiding the vulnerabilities or by protecting information that makes individuals vulnerable.[69] Nevertheless, the concept of privacy is not thoroughly defined and it is not clearly understood how the relation between privacy and vulnerability unfolds.

In what follows, I will show that the relationship between privacy and vulnerability is determined by their concern with autonomy. What is more, I will argue that incorporating a thick understanding of privacy into the concept of digital vulnerability can help to balance the hypo-autonomy of consumers against the hyper-autonomy of companies in the digital sphere ex ante. This strengthening of the consumer position is possible because *thick privacy* allows us to see *why* consumers are less autonomous in the digital sphere than in other spheres of consumer action: because the hyper-autonomy of companies is based on large-scale surveillance and privacy-intrusions. These violations of privacy are the very basis of vulnerability, because they inhibit the *formation* of autonomous will, which then later have an impact on the *expression* of that will (distortion of economic beha-

65 Helberger et al., *supra* note 16, 190.
66 Galli, *supra* note 16, 199.
67 Helberger et al., *supra* note 16, 190.
68 Ryan Calo, *Privacy, Vulnerability, and Affordance*, 66 DePaul Law Rev. 591–604 (2017), 596.
69 ibid., 600.

viour). *Thick privacy* emphasizes the conditions for autonomy. Autonomy needs privacy. Privacy is a necessary conditions for autonomy because it protects a physical or – in the digital world – a mental space in which individuals can develop and reflect on values which they deem to be their own.

I. The value of privacy

Here, I follow those authors who attribute a distinct value to privacy as opposed to the ones who see privacy merely instrumental to other values. Already Brandeis and Warren, the arguably first ones to define the right to privacy, attribute a coherent and distinctive value to privacy which they conceptualize as the right to be left alone.[70] This stance was later defended by several authors. Bloustein, for example, saw a distinct value in privacy has– connected to human dignity - that would get lost if it wasn't mentioned.[71] Also Gavison sustains that privacy should be legally protected in itself because or even though serves different important functions (human aspirations).[72] And Inness attributes a distinct value to privacy because it embodies our respect for peoples are creators of their own plans of intimacy and emotional destinies. For her, intimacy is the core of privacy, which has to be distinguished from other interests such as the right to be let alone or the freedom from government intervention.[73]

Fried understands privacy as being important for a human space and argues that privacy is a moral value in itself that goes beyond being merely a tool for assuring another substantive interest.[74] It is rather the foundation without which other fundamental ends and relations (respect, trust, friendship, love) would simply not exist. Relationships build on common moral perceptions of personality, basic entitlements and duties vis-à-vis each other. Without privacy, the very integrity of humanity and personhood would be threatened and without privacy and we would not be human at all.[75]

70 Samuel D. Warren & Louis D. Brandeis, *The right to privacy*, 4 Harv. Law Rev. 193–220 (1890).
71 Edward J. Bloustein, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, 39 New York Univ. Law Rev. 962 (1964).
72 Ruth Gavison, 'Privacy and the Limits of Law' (1984) 89 Yale Law Journal 421, 425.
73 Julie Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press 1992), 74 ff.
74 Charles Fried, 'Privacy' (1968) 77 The Yale Law Journal 475, 477.
75 ibid., 477.

Privacy is essential to all human relationships because without respect for privacy, the minimal precondition for any relation would be missing.[76] For example, there would be no trust where there is no possibility of error that a private space provides.[77]

Gavison shows that scholars who argue that privacy does not have inherent value usually derive this argument from judicial decisions that usually do not protect privacy alone but in connection with another value and, thus, push them towards assuming no overarching value in itself.[78] However, she shows that the one does not logically follow from the other. Moreover, the instrumental view neglects the motivations for individual privacy claims.[79] Finally, as reductive accounts 'suggest that privacy is only a label used to protect other interests, logic would dictate that whenever a privacy question is discussed, the balancing should be among the "real" interests involved. Consequently, privacy is made redundant despite its usage.'[80]

For our purposes, it is important to see that the inherent, and if you wish: moral, value of privacy derives from the function of privacy. Privacy enables other values, such as autonomy, mental health, creativity, the capacity to create meaningful human relations, or even the formation of liberal citizens. These functions should not be understood in a modal way. Rather, these positive functions of privacy relate to the promotion of liberty, moral intellectual integrity, intimate relationships, and ideals of a free society in a law-like way, similarly to a *conditio sine qua non*.[81]

II. *Thin privacy* in EU Law: control rights

There are what I would call thin and thick accounts of privacy. The former operate more on the surface-level of observable behaviour, the latter provide context and deeper meaning to the concept of privacy. In the EU, the understanding of privacy is thin one. It is highly limited and, in the commercial sphere, is reduced to data management rights.

76 ibid., 484.
77 ibid., 486.
78 Gavison, *supra* note 72, 461-463.
79 ibid., 465.
80 ibid.,. 467.
81 Jeffrey L Johnson, 'A Theory of the Nature and Value of Privacy' (1992) 6 Public Affairs Quarterly 271, 280.

First of all, privacy protection does not have to be a concern for the commercial sector. The right to privacy as protected under Article 8 ECHR is not generally applicable in horizontal relations. While the ECtHR has carved out the right to privacy in the ECHR, arguably covering a wider range of interests, such as private and family life, home, and correspondence, right to one's imagine, identity and personal development, as well as the right to establish and develop relationships with others, the protection afforded under Article 8 ECHR does not have direct effect for the relations between consumers and companies that surveil them.

Second, in the commercial realm, privacy is understood in a limited way as data protection. The GDPR outsources the issue of privacy protection to the ePrivacy Directive 2002/58,[82] which focuses more narrowly on electronic communication and the use of cookies and other trackers. It is currently in the process of being reformed by the draft ePrivacy Regulation (ePR),[83] as part of the protection regime demanded by Article 7 ChFR, focusing on the confidentiality of electronic communications generally. The GDPR, in turn, regulates the use of personal data. It conceptualizes privacy merely as a set of control rights. The GDPR contains a catalogue of rights, which data subjects can exercise or not, such as the right to transparent information about data processing, Articles 11 through 15 GDPR, right to rectify wrong data, Article 16 GDPR, the so-called right to be forgotten, Article 17 GDPR, the right to restrict processing, Article 18 GDPR, or the right to object, Article 21 GDPR. Moreover, data collection and processing are only lawful if it is based on consent or necessity, Art 6 GDPR. Taken together, these provisions reflect a regulatory approach to privacy protection that is based on individual action by the data subject. It is the data subjects who have to give consent to data collection and processing and then take action in case there is wrong data or in case they want to object to data processing or erase data. Without such action, data collection and processing can and will proceed undisturbed. The approach to consent in the draft ePrivacy Regulation is the same, see Recital 18 ePR.

82 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

83 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

Even though onsent as the main legal basis for lawful data collection and processing has recently been strengthened in the case of *Meta v Bundeskartellamt* through stricter requirements for consent as a legal basis and for circumventing it by business 'necessity',[84] the interplay of consent and data rights in EU law reduces privacy to data control rights. They are personal data management rights. The protection under the GDPR can be called Do-It-Yourself protection,[85] which only gives weak power to individuals that cannot match the power of digital companies.[86] *The Meta*-judgment does not touch upon discussions to what extent the GDPR actually contains many pitfalls and hindrances to actual effective control.[87] The judgment about conceptual limitations of the GDPR comes *ante* the assessment of its effectiveness. This approach is in line with the general concern of the GDPR, which is not privacy or data protection per se, but rather the establishment of an internal data market. The GDPR does lay down rules for the protection of individual data (Article 1 (1) GDPR), but does so within the context of its aim to create an internal data market (Article 1 (3) GDPR). It includes rights that clearly serve the establishment of an internal market: for example, the right to data portability, which is inherently concerned with the movement of data from one provider to another. Recital 13 GDPR even states that the 'proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.' This statement makes it clear that the internal market comes first; data protection second.

This outline shows that, in EU consumer law, privacy is understood in a narrow way. Data serves as a proxy for privacy and individuals are put in charge of its protection. The EU understanding comes close to

84 Case C-252/21 *Meta Platforms Inc. Meta Platforms Ireland Ltd, Facebook Deutschland GmbH v Bundeskartellamt*, ECLI:EU:C:2023:537.

85 Alec Wheatley, 'Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation With a Private Right of Action' (2015) 45 Golden Gate University Law Review; Tobias Matzner and others, 'Do-It-Yourself Data Protection—Empowerment or Burden?' in Serge Gutwirth, Ronald Leenes and Paul De Heert (eds), *Data Protection on the Move - Current Developments in ICT and Privacy/Data Protection*, vol 24 (2016).

86 Daniel J Solove, 'The Limitations of Privacy Rights' [2022] GW Law Faculty publications.

87 I. van Ooijen & Helena U. Vrabec, *Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective*, 42 J. Consum. Policy 91–107 (2019).

privacy as the control over information, more specifically how and to what extent personal data should be collected and processed for business purposes. Control is exercised through the granting or denial of consent and rights concerning rectification, erasure, mobility, or objection. This is a thin understanding of privacy in terms of control rights is concerned with authorization as the variable that decides on the lawfulness of publication of information. Privacy gives the right to control information, as Westin claimed in 1967,[88] meaning the individual right to determine when, how and to what extent information about them is communicated. This includes the right to withhold or conceal information (privacy as secrecy).[89]

III. *Thick privacy*: substantive dimensions

There is a spectrum of thicker accounts of privacy. On one end of the spectrum, we can locate ideas of privacy as clear boundary-setting between a private self and public intrusion. On the other end, emphasis is put on the context-specific construction of a private sphere.

An example of the first group is the Warren and Brandeis' right to be left alone,[90] which draws a strict line separating private and public behaviour. They are not interested in what it is that precisely makes certain behaviour private or public. What matters for them is the idea that 'something private' is being 'made public.' While emphasis is on the movement from the private into the public without consent, thus basing themselves in the idea of control, it could provide grounds for a thicker understanding of privacy because it is absolute. In the context of the rise of 'mass media and newspaper enterprise, instantaneous photographs, gossip as trade at the end of the 19th century, Warren and Brandeis' privacy is the necessary 'retreat from the world'.[91] It includes the idea of an inviolate personality.[92] In a similar vein,

88 This is probably the most wide-spread understanding of privacy. Fundamentally: A. Westin, *Privacy and Freedom* (London: The Bodley Head 1967).

89 See R. Posner, "The Right of Privacy" 12. *Georgetown Law Review* 1977, p 393. For an overview of different definitions, see D. Solove, "Conceptualizing Privacy" 90. *California Law Review* 2002,1087.

90 Warren and Brandeis, *supra* note 70.

91 ibid., 195-196.

92 ibid., 205.

other authors define privacy as the limited access to a person.[93] They share a concern for a certain boundary that needs to be defended. Privacy refers to the right to determine the boundaries of an own private – as opposed to public – space. This approach can be called defensive because of its role in protecting a personal space of liberty in which the very self can flourish.

An even thicker account of privacy is provided by Cohen who defines privacy as freedom from surveillance.[94] She sees privacy as foundational for informed and reflective citizenship on the one hand and the capacity for innovation on the other. For her, privacy protects 'the situated practices of boundary management through which the capacity for self-determination develops.[95] While the idea that privacy protects the space for the development of the liberal self has an aspect of boundaries to it,[96] Cohen's concept of privacy is thicker because she is concerned with shelter emergent subjectivity from efforts of commercial and governmental actors to render individuals transparent and predictable'.[97] Surely, privacy as a shield is about control of those boundaries, but it is also about the defence and preservation of a space in which the will to control can even develop. As 'emergent subjectivity' exists in the space between the experience of autonomy and social shaping, Cohen acknowledges that the 'self' is socially constructed.

Similarly, Solove argues that privacy cannot and should not be defined in a static way, but always in relation to a specific context. Privacy, in this view, refers to the practices (activities, customs, norms) that are the product of history and culture.[98] It cannot be understood a priori but only in specific contexts of social practices. The protection of privacy implies the protection of those social practices from disruption. Against the backdrop of historically changing conceptions of privacy, the value of privacy in each and every specific situation is also changing. For Solove, the value of privacy *in the context of large-scale surveillance* lies in the protection from

93 Hyman Gross, *The Concept of Privacy,* 42 New York Univ. Law Rev. Also Gavison, *supra* note 73.

94 Julie E. Cohen, *What privacy is for*, 126 Harv. Law Rev. 1904–1933 (2013), 1905.

95 ibid., 1905. also: Cohen, "Configuring the Networked Self: Law, Code, and the Play of Everyday Practice" *Gergetown Law Faculty Publications and Other Works*, 2012, p 149.

96 Cohen, *supra* note 94.

97 ibid., 1905.

98 Daniel J Solove, 'Conceptualizing Privacy' (2002) 1087 The Individual and Privacy: Volume I 333, 1092-1093

a systemic oppressiveness that suffocates the exercise of power that renders people vulnerable and helpless.[99]

Acknowledging the pervasiveness of the digital surveillance architecture, Ienca and Andorno introduce the concept of mental privacy as a 'neuro-specific' right that copes with possible misuses of neurotechnology and its threat to fundamental liberties associated with individual decision-making.[100] To them, privacy protection in this context implies the recognition of a negative right to cognitive liberty that protects individuals from the coercive and unconsented used of neuro-technologies as well as the right to mental privacy and the right to psychological continuity. The right to mental privacy protects 'private or sensitive information in a person's mind from unauthorized collection, storage, use, or even deletion in digital form or otherwise, thus protecting not only *expressed information* but also the *generation* of such information. The right to psychological continuity, in turn, protects the 'mental substrates of personal identity from unconscious and unconsented alteration by third parties' through the use of neuro-technologies. Their idea goes significantly beyond the ideas expressed above (thin privacy) as it incorporates a concern for the pervasiveness of new technologies. In this way, it gives shape to the concern shared with Cohen and Solove about the mental effects of large-scale surveillance.

To my mind, Ienca and Andorno synthesize the interpretations of privacy specifically for the digital sphere. It is the probably thickest of all accounts of privacy because it does not merely deal with the expression of internal will but also with the possibilities of its formation. It gives another name to Cohen's protection of emergent subjectivity. Moreover, it shows that accounts such as Fried's or Inness' – which are concerned with attributing inherent value to privacy - are very well applicable in the digital sphere. Despite Solove's critique of attempting of finding an overarching definition, Ienca and Andorno's critique of dismantling of intimacy or other conditions for any human relation and activity is spot on in the context of large-scale surveillance. In my view, their ideas can be reformulated in Solove's terms not as overarching definitions but as a concern for the preservation of a shelter for human flourishing *within the specific context* of large-scale supervision in the political economy of informational capitalism. Both Fried's and Inness' concern for the inherent function of privacy

99 ibid., 1149 ff.

100 Marcello Ienca & Roberto Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, 13 Life Sci. Soc. Policy 1–27 (2017).

for intimate human relationships and Cohen's freedom from surveillance as a pre-requisite for 'protected zones of personal autonomy aim at giving room to productive expression and development to flourish'.[101] Mental privacy is the specific privacy that is protected by freedom from surveillance.

IV. Privacy and autonomy

There is a necessary connection between privacy and autonomy because privacy is pivotal for autonomy. I have elaborated on this connection in more detail elsewhere, based on the model of informed consent by Faden and Beauchamp,[102] so I will confine the following to a summary of the points that are important for this contribution. To Faden and Beauchamp, autonomous action must be intentional, based on understanding, and free from controlling influences.[103] Intention arguably develops in condition of privacy because it is concerned with the formation of authentic will, while the freedom from manipulation concerns the expression of will. Faden and Beauchamp are weary of including authenticity of will as an additional requirement for autonomous action because they believe that it would narrow down the scope of actions protected by a principle of respect for autonomy.[104] For them, it makes sense to define 'autonomy' broadly and not include too many limiting parameters (such as authenticity). Their concern is, thus, with casting a broad net in order to lead to broad protection of what can be considered autonomous action.

For our purposes it is however useful to include a notion of authenticity into the 'intention' parameter of their informed consent theory. It allows us to cast a wide net over what would have to be protected in large-scale surveillance. For the aim of highlighting the importance of privacy for autonomy, it makes sense to include authenticity into the conceptual framework of what *intention* is, because in case of its absence, we can determine a violation of the conditions for autonomous action and informed consent. Here, including privacy conditions leads to a wider 'surface' to catch more

101 Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stanford Law Rev. 1373 (2000),1377.

102 Irina Domurath, 'Plaform Economy and Individual Autonomy' (2022) 30 European Review of Private Law, with reference to Ruth R Faden and Tom L Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press 1986).

103 Ruth R Faden and Tom L Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press 1986), 238.

104 ibid., 265.

possible violations. In the end, this result is in line with the goal of broad the protection sought by Faden and Beauchamp (who made their argument before the emergence of pervasive new technologies).

The connection between privacy and autonomy is either explicit or underlying the above-mentioned definitions of privacy. In the defensive accounts of privacy as a space of non-interference, the protection from any type of intrusion is considered incompatible with the freedom associated with a personal space in which the self can develop and flourish. Also Westin is concerned with this space. He sees the preservation of autonomy goal of privacy protection, a release from role-playing, and the possibility of having time for self-evaluation and for protected communication.[105] Autonomous individuals can exist only when there is the possibility of establishing a boundary between the self and their surroundings. Total transparency – the complete lack of privacy –signifies the disappearance of the boundary between the self and its surrounding; a 'transparent self' cannot exist because individuation needs a certain amount of concealment from the environment.[106]

A more substantive connection between privacy and autonomy can be found in Cohen's understanding of privacy regards freedom from surveillance. Here, privacy as the absence of surveillance is foundational to the practice of informed and reflective citizenship, and therefore an indispensable structural feature of liberal democratic political systems.[107] To her, a lack of privacy means a reduced scope for self-making (along liberal or other lines) through the development of subjectivity that is shaped by social and communal values.[108] She focuses on the conditions for 'meaningful autonomy in fact'.[109] Thus, the right to be left alone must, in a political economy of informational capitalism that is based on large-scale surveillance, comprise the right to be left alone *mentally*. It implies the right to not merely control, but close off a mental space for any intervention or influence of any kind, including nudging and other attempts of behavioural manipulation. It is precisely this space free from intervention and observation that is needed for play, experiments, successes and failures as necessary

105 A. Westin, *Privacy and Freedom* (London: The Bodley Head 1967).
106 Ida Koivisto, *The Anatomy of Transparency: The Concept and its Multifarious Implications*, EUI Work. Pap. MWP 1–22, 20 (2016).
107 Cohen, *supra* note 94, 1905.
108 ibid., at 1911.
109 Cohen, *supra* note 101.

for the development of individual personalities, which, in turn, is the basis for any human interaction, be it personal, social, economic, or political.

This does not mean that individuals need to be completely disconnected from their surroundings in order to be autonomous. For our purposes, it is not important whether autonomy thrives only in the possibility of complete seclusion from any societal forces or whether autonomy is constitutively shaped by interpersonal relations and interactions, because large-scale surveillance undermines both, the secluded individual and the socially and culturally shaped individual. Emphasizing the possibility for a mental space as a necessary condition for autonomy rather than the conditions under which individuals acquire their identity makes this clear. If we regard individuals only as autonomous in the complete absence of any influence – the broader protection would be afforded here -, autonomy is eroded because there is no mental space under large-scale surveillance. If we regard individuals as socially constituted and shaped, autonomy is also eroded because there is no mental space either for developing basic autonomy. There is nothing that social factors could even influence and help to shape. Big data analyses, data mining, and deep data are ever more intruding upon the internal space where freedom of thought, free will, and individual autonomy can develop. Surveillance deprives private autonomy of its very foundation because it runs counter to the idea of a mental space for its development.

V. Interim conclusion 2

Privacy has an intrinsic value as the basis for individual autonomy. The current EU Law framework falls short of this understanding because it outsources privacy-concerns to the public sphere in which states and public authorities must be held accountable for privacy intrusions, whereas only giving data management rights to individuals in the commercial sphere. Those rights merely serve to control data flows, giving consumers very little power vis-à-vis companies who collect, exploit, and sell that data. In this way, EU Law incorporates a thin understanding of privacy.

In contrast, the concept of thick privacy draws our attention to large-scale surveillance on which digital business strategies are based. Understood as freedom from surveillance or mental privacy, *thick privacy* for the digital sphere emphasizes that individual autonomy is not merely attacked by manipulation, but is structurally and inherently eroded. Acknowledging

that privacy – including mental privacy – is a necessary conditions for autonomy and the formation and exercise of any meaningful informed consent in practice, shows that the mere monitoring of consumer behaviour is a violation of privacy that can inhibit consumer autonomy to develop in the first place. As a consequence, the conditions for informed consent – the basis of consumer dealings in the digital sphere – are not met.

D. Conclusion: digital vulnerability and thick privacy

Digital vulnerability is a new type of consumer vulnerability related to the emergence of new digital technologies. Hitherto, it describes the potential for harm through the adaptive persuasive systems employed in digital or algorithmic marketing. *Digital vulnerability* has the potential to move EU law away from its static understanding of consumer vulnerability in variation from the benchmark consumer standard to a more substantive understanding of vulnerability in the digital economy. This can be evidenced by the proposals put forward, for example by Helberger et al. They suggest a variety of changes based on *digital vulnerability* intended to improve the information paradigm by implementing an obligation for personalized privacy notices, consent as a process, as well as more efficient teaching and training programmes.[110] Moreover, they show that the structural asymmetries between companies and consumers in the digital economy (digital asymmetry) can qualify as forbidden 'aggressive practices' under Articles 8 and 9 UCPD, while being subject to a last resort fairness check under Article 5 (1) UCPD.[111] Similarly, Galli argues that Article 5 (1) and (2) UCPD create new professional duties and obligations of professional diligence, such as privacy by design, and that the digital-choice environment could qualify as 'undue influence' under Article 9 UCPD.[112]

To my mind, these proposals do not go far enough. The concept of digital vulnerability can do more than enable new interpretations. In fact, the mentioned proposals become substantially weaker as soon as there is talk of 'broader societal developments' that 'have to be taken into account'. For example, Helberger et al, when advancing better media literacy proposals, acknowledge that 'not including a broader social perspective and not ad-

110 Helberger et al., *supra* note 16, 41 ff.
111 ibid., 49 ff.
112 Galli, *supra* note 16.

dressing the inequalities of power and knowledge mentioned … renders this effort insufficient for protecting consumers in the online environment.'[113] But this is not followed by clarifications about how those inequalities of power and knowledge could and should be addressed.

Viewing vulnerability as a power relation, shifts our focus towards the main constituent parameter of this power asymmetry: autonomy asymmetry. On the one hand, there is the *hyper*-autonomy of digital companies: the structural power to determine not only their dealings with consumers but also the environment in which these dealings take place. Companies are the ones who make the very markets on which they all other market players interact. They make those markets through large-scale surveillance, collecting vast amounts of data, and turning profits through personalization. On the other hand, there are the *hypo*-autonomous consumers, unable to negotiate their dealings with companies and certainly not to build the markets on which they interact with companies.

Adopting the notion of *thick privacy* – understood as mental privacy and freedom from surveillance - for the concept of digital vulnerability would give substance to this power relation. While both Helberger et al and Galli do give a lack of privacy a role to play in the creation and manifestation of digital vulnerability, both accounts under-conceptualize privacy. It is however here, where the concept of digital vulnerability could unfold its potential. Privacy impacts upon digital vulnerability precisely because it secures the conditions for autonomy. Privacy protects autonomy. Digital vulnerability reflects diminished consumer autonomy.

If the literature on digital vulnerability made it clear that privacy needs to be understood in a thick way, privacy intrusions through large-scale surveillance could be adequately included into the concept of digital vulnerability. In Helberger et al.'s version, the incorporation of *thick privacy* would emphasize the state of universal defenceless in exposure to power imbalances. This defencelessness would not – as they claim - merely be precipitated by the automation of commerce, datafied selling relationships and general digital architecture, but would specifically derive from large-scale surveillance. Adopting a thick understanding of privacy would explain why the digital architecture does in fact lead to vulnerability: because privacy is invaded structurally through mental monitoring, measuring, and manipulating. In Galli's layered digital vulnerability, the acknowledgement of *thick privacy* would let collapse the distinction between the foundational layer of

113 Helberger et al., *supra* note 16, 44.

the architecture of algorithmic marketing and the second layer of privacy. The large-scale invasion of privacy is part of the architecture of algorithmic marketing.

Thick privacy changes the focus of both the digital vulnerability concept and the consumer vulnerability framework in EU Law away from the manipulation of behaviour (the expression of autonomy) towards a much more subversive change of thinking and manipulation of will (the formation of autonomy). Large-scale surveillance – this is the contribution of *thick privacy* – impedes self-determination at the most basic level. The focus on the economic distortion of consumer behaviour through manipulation comes in at a later stage, when avoiding economic and financial harm from the subversively manipulated will of consumers. *Thick privacy* in a context of surveillance capitalism makes it clear that economic and financial harm in terms of behavioural manipulation is merely a symptom of the underlying harm to the formation of self-determination and free will. In this way, the concept has the potential to balance the hypo-autonomy of consumer against the hyper-autonomy of companies. Thick privacy can be used as a sword[114] also by consumers because it makes it clear that it is large-scale surveillance and data collection that makes them vulnerable. In this way, the violation of *thick privacy* thus becomes the root of digital vulnerability. Adopting a thick idea of privacy within a concept of digital vulnerability (and hopefully into EU Law) would thus shift our focus away from emphasizing the danger for manipulation of consumer behaviour to a state prior to the actual decision-making, namely the formation of consumer will.

114 Calo, *supra* note 68.

Digital Vulnerability and the Formulation of Harmonised Rules for Algorithmic Contracts: A Two-Sided Interplay

Teresa Rodríguez de las Heras Ballell

A. Setting the scene and delineating the scope: automated decision-making

Algorithmic and AI-driven automation has pervaded an immense and growing variety of tasks, activities, and decision-making processes in the digital economy. From basic tasks (searching, comparing, ordering, prioritizing, ranking), to more sophisticated added-value services (profiling, personalizing, recommending, multi-attribute rating, filtering, content moderation, algorithmic management, complaint handling, negotiation, automatic adjustment of conditions), they are performed by algorithm/AI-driven systems.

The benefits of efficiency, rapidity, personalization, and cost-reduction have also encouraged the use of algorithmic/AI systems for contractual purposes throughout the entire contract life-cycle: from the negotiation phase to the performance of obligations, termination and enforcement - digital agents; virtual assistants; chatbots; smart products; self-executed smart contracts; personalized transactions; 'dynamic contracts'; automated renegotiation, termination and self-enforcement of agreed consequences for default.

The notion of algorithmic contracting intends to encapsulate all these use cases where algorithmic/AI systems are employed to automate any (one or several) stage/s of the contract life-cycle – from preliminary dealings to termination and enforcement. This intersection between automation and contractual purposes draws the perimeter of the phenomenological scenario for this Paper to test the notion of 'digital vulnerability' and to propose the (sub-)variant of 'algorithmic vulnerability', which is coined, to surface such vulnerabilities specifically stemming from the use of automated decision-making systems (hereinafter, ADM).[1]

1 ELI *Guiding Principles for Automated Decision-Making in the EU*, at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf.

The premise of this Paper is that the use of ADM for contractual purposes raises issues that trespass and exceed the perimeter of the solutions devised for enabling electronic commerce.

The sentiment that the use of ADM and AI systems in and for contracting implies a new stage in the evolution of contracting forms and contractual practices that goes beyond the challenges of electronic contracting has mobilised not only doctrinal reflection, but also attracted the attention of legislators and regulators on the international scene. The prevailing need to understand the scope of this phenomenon, to assess its implications on existing principles and rules and, where appropriate, to propose specific solutions to mitigate its risks without hindering its penetration in commercial activity or stifling its benefits has prompted study initiatives, proposals for principles and legislative actions in various fora.

The United Nations Commission on International Trade Law (UNCITRAL), whose instruments on electronic commerce have been essential and instrumental in consolidating a body of uniform principles for the first electronic revolution, has embarked, in its Working Group IV on Electronic Commerce[2] , on a project on AI and automation in international trade. In accordance with the mandate received, the group compiled existing provisions in relevant UNCITRAL texts, assessed their suitability for automated contracting and was expected to develop, to the extent necessary, a set of principles[3] and provisions to provide legal certainty for the use of AI systems in the negotiation, conclusion, performance and enforcement of an international contract. At the 57th UNCITRAL Commission session held in New York in July 2024,[4] the work of the WG IV concluded with the adoption of the Model Law on Automated Contracting (hereinafter, MLAC). Thus, UNCITRAL contributes to provide legal certainty for the development and the use of AI to form and perform contracts in international trade.

2 The author is the Spanish Delegate to the United Nations (UNCITRAL, United Nations Commission on International Trade Law) in Working Group IV. All opinions expressed in this paper are personal to the author.

3 The current status of the project and session documents are available at https://uncitral.un.org/es/working_groups/4/electronic_commerce.

4 See https://unis.unvienna.org/unis/pressrels/2024/unisl363.html.

The *European Law Institute* (ELI) issued in 2022 a set of principles for the use of ADM systems[5] (hereinafter ELI *Guiding Principles for ADM*) on which is based the ongoing project on Algorithmic Contracts[6] (hereinafter, ELI *Project on Algorithmic Contracts*) which has started analysing European consumer protection law to assess its adequacy and sufficiency for the use of AI systems in consumer transactions and is in the process of developing a set of principles and model rules for algorithmic contracts with special focus on B2C transactions.

These initiatives are clearly aimed at addressing the legal issues raised by algorithmic contracts with a Private Law approach. But they must also be framed within an expanding universe of norms, recommendations, principles and standards on AI systems that, while not necessarily connected to their use in and for contracting, underpin an increasingly dense regulatory space for the development, implementation and use of AI systems in a socioeconomic context. The AI Regulation (or AI Act) [7] is, in this sense, the most ambitious EU text to lead the building of a regulatory and legislative framework for AI. The AI Act is not designed to govern algorithmic contracts, but it crystalizes several policy decisions and provides for requirements and legal solutions that may transpire increasing global consensus on certain legal standards.

Besides, the AI Act, albeit being the globally recognized landmark of the EU response to AI governance and regulation, it is not in a vacuum and it is accompanied by other important legislative actions aimed at addressing the multifaceted challenges of AI. In fact, the European Union has embarked on an ambitious initiative[8] to review and adapt the regulatory framework

5 *ELI Guiding Principles for Automated Decision-Making in the EU*, available at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf.

6 *ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts*, Ongoing Project - https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/.

7 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), PE/24/2024/REV/1. OJ L, 2024/1689, 12.7.2024.

8 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe, COM*(2018) 237 final; Commis-

to the digital economy and, in particular but not only, to AI. The two proposals for a Directive on AI liability – Proposal for a Directive on the adaptation of non-contractual civil liability rules to artificial intelligence[9] (AILD) – and for a revision of product liability rules - Proposal for a Directive of the European Parliament and of the Council on liability for defective products[10] (revPLD) - illustrate how this process of modernisation and adaptation has a direct impact on key parts of the private-law system.

The under-construction, changing and still uncertain, above-described legal environment sets the stage for exploring the polyhedric concept of 'digital vulnerability'. As a starting point, the interplay between the rules for algorithmic contracts and the notion of digital vulnerability shows two angles.

Within the scope of the UNCITRAL work, the digital vulnerability does not seem to play a remarkable role, even more, it might be deemed absent in the approach and the deliberations. In consistency with its mandate for harmonizing rules for international trade, acknowledging forms of vulnerability would arguably shift the focus to areas out of the reach of the UNCITRAL's scope. It is not the emergence of vulnerabilities what triggers

---

sion Staff Working Document, *Liability for emerging digital technologies* - Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, SWD(2018) 137 final; *Ethics Guidelines For Trustworthy AI* from the High-Level Expert Group on Artificial Intelligence, 8.4.2019; White Paper on Artificial Intelligence - *A European approach to excellence and trust, COM(2020) 65* final, Brussels, 19.2.2020; Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, *Report on the implications of artificial intelligence, the Internet of Things and robotics for security and liability,* COM(2020) 64 final, Brussels, 19.2.2020; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM(2020) 67 final, Brussels, 19.2.2020. The creation in 2018 of the *Expert Group on Responsibility and New Technologies,* divided into two formations: New Technologies Formation and Product Liability Formation. The New Technologies formation published its report in November 2019 *Report on Liability for Artificial Intelligence and other emerging technologies* (https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en).

9 COM/2022/496 final.

10 COM/2022/495 final. P9_TA(2024)0132. European Parliament legislative resolution of 12 March 2024 on the proposal for directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)).

the need for harmonizing rules for the use of AI in international trade, but legal uncertainties and jurisdictional disparities that hamper cross-border transactions. The idea of vulnerability appears, in the international legal harmonization discourse, anchored in consumer-protection considerations that fall outside the remit of 'uniform law for international trade'. To that extent, in the deliberations and in the draft solutions of the UNCITRAL WG IV's work, concerns for digital vulnerability arising from algorithmic contracting is not transpired. In the adopted MLAC, only incidentally in the basic rules of legal recognition or attribution concerns about the vulnerability inherent to the 'automated contracting' may be glimpsed. A specific rule, incorporated as an optional (in brackets) provision, on unexpected actions or decisions of the automated system (Art. 9 MLAC) is probably the only, and most, visible, albeit attenuated by its reinforced optional character for States,[11] permeation of vulnerability considerations in the UNCITRAL text.

Thus, a very dim notion of vulnerability might be glimpsed in the formulation of uniform rules of algorithmic contracting in international trade if it is understood as revealing any situation of asymmetry or inequality in the allocation of risks. From this faded concept of 'vulnerability', it would be possible to affirm that in the formulation of rules that provide certainty, unpredictability, and clear solutions in the attribution of legal effects, the allocation of the risks of errors, unexpected actions, or malfunctioning, or the distribution of liability's consequences, there is actually a perception that the use of ADM (specially, AI-enabled ADM systems) in the contractual process creates new balances or imbalances between the parties that if they remained unresolved or wrongly managed, AI-enabled trade would be disincentivised. It might be argued that uncertainties on the validity and enforceability of AI-performed actions and decisions, the allocation of risks, and the exposure to liability when using ADM systems bring about vulnerabilities that uniform rules aim to prevent or contain. Even at risk of appearing to be a strained interpretation of the notion of vulnerability, it helps to appreciate that the solutions adopted in the formulation of harmonized rules for AI international trade contributes to the discussion and the calibration of digital vulnerability beyond its scope, including in

11 A/CN.9/LVII/CRP.9 As a model law, States can adopt fully or partially, modify, or not incorporate any provision of the text. Additionally, Article 9 is included in the text in brackets with a footnote advisinfg that "This provision is included for States wishing to enact one or more specific provisions addressin unexpected actions carried out by automated systems".

consumer contracts. Thus, as an illustration, whether the policy decision followed on the allocation of any risks lies in the operator (deployer or user) of the ADM under all circumstances, operators (and, primarily, consumers) are now exposed to a new form of vulnerability that may require a reversal or containment.

Accordingly, regardless of the strong or weak notion of vulnerability that is accepted, the assumption that the basic rules on algorithmic contracting solving the key issues on validity and enforceability, attribution, allocation of risks or liability set the scene where to test and on which to build up a concept of digital vulnerability (narrowed down to 'algorithmic vulnerability') is the backbone of this Paper. Two rules, in particular, are crucial in building a solid framework: legal recognition and attribution (II). Other rules on allocation of errors, or the attribution of unexpected outcomes are also essential and should be studied in depth (but they are not covered in this Paper).

Contrariwise, the ELI project, notably in its first output (ADM-readiness test of EU Consumer acquis),[12] is amply permeated by the acknowledgement that algorithmic contracting (with consumers) creates (or aggravates) new forms of inequality and ADM-specific solutions may be needed for mitigating vulnerability risks. This is the first angle of the interplay between digital vulnerability and algorithmic contracting. A positive correlation that intensifies the vulnerability risk. In this regard, this Paper proposes a narrower notion as a sub-type of digital vulnerability that solely captures the specific challenges stemming from the use of ADM (and not in general from the digital context): it is named 'algorithmic vulnerability'. But the second angle of the interplay between algorithmic contracting and the notion of digital vulnerability provides an inverse perspective. The use of ADM in contracts, specially by consumers, has the potential to revert traditional paradigms, attenuate asymmetries, and repair failures. Consumers might be less vulnerable if assisted by ADM systems. If so, interestingly, new forms of vulnerability emerge when consumers are deprived of the possibility to use such assistive systems, if such a use is prevented, hindered, or rendered unfeasible by traders (by implementing commercial practices, by design of interfaces, or by contractual terms). Hence, countering such

12 *Interim Report, EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* 2023, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.

vulnerability-aggravating situation might require specific provisions aimed at enabling the use, facilitating their operation, and prohibiting (or discouraging) impeding practices, blocking measures, discriminatory terms, or ADM-unfriendly interfaces.

The Paper is structured in four parts including this scene-setting and introductory section. Under this introduction (A), there are two sections, First, section I defines algorithmic contracting, while section II maps the scenarios covered by the notion. The second part (B) identifies and explains the main legal issues arising from algorithmic contracting ranging from the attribution of legal effects to the allocation of liability. This mapping exercise of the main legal issues that algorithmic contracting raises invites the discussion on their interaction with the notion of digital vulnerability. It explores the (two) main legal issues arising from the use of ADM in and for contracting to learn whether it exacerbates, or even have any effect on, vulnerability risks or create new forms of inequality throughout the contract life cycle in commercial transactions. This initial question will be followed by a subsequent one (C) that is focused on consumer contracts to discuss whether consumers are better protected or more vulnerable instead in algorithmic contracts. In examining consumer legislation throughout the lens of algorithmic contracting, some paradigms need to be revisited in the light of new balances and risks triggered by the use of ADM systems in contracting contexts, or at least the rationale behind current safeguards may invite reconsideration. While unveiling and calibrating vulnerability risks raised by algorithmic contracting, it will be discussed whether algorithmic contracting does always and irremediably exacerbate digital vulnerabilities or whether it can reverse or curb this presumed and purportedly inevitable consequence by repairing failures and re-equilibrating asymmetries. If so, which are the sources of these vulnerabilities that are labelled as 'digital' and, therefore, which is or are the triggers. Yet, the next step is to assess whether the existing legal and regulatory framework is suited to prevent these digital vulnerabilities and contain their undesired effects. All these final remarks are summarized in the last part (D).

I. Defining algorithmic contracts

The choice of the term (algorithmic contracts and algorithmic contracting) for the purposes of this Paper is not free of objections and constraints,

but there are reasons to endorse its use as reasonable and sufficiently convincing.

'Algorithmic contracting' succeeds in conveying the key elements of the problem to address and in delimiting the contours of the scope. The focus of the Paper is on the use of algorithmic/AI system for contractual purposes at any of the stage of the contract life-cycle. In this regard, the algorithmic/AI system is employed to take a decision or in relation to a decision-making process. Therefore, algorithmic/AI systems, ADM systems, automated systems, and, to a certain extent, automation, and consequently automated contracting and algorithmic contracting, are terms interchangeably used throughout the Paper.

Algorithmic contracting refers to a diversity of phenomenological scenarios where one or both parties use ADM systems (algorithmic/AI systems for decision-making) for purposes related to the negotiation, formation, performance, or enforcement of a contractual agreement. To that end, the term seems appropriate and revealing as it does visibly interconnect the two components of the targeted subject matter.

First, the technological component (automation). It comprises the use of both deterministic algorithmic systems and AI-driven learning systems.[13] The term does not prejudge any technology and, in that regard, it aims to be technology-neutral and model-agnostic. Foundational models[14] are separately defined and subject to specific risk classification and requirements.

13 Article 2.(1) AI Act:
AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;.

14 The AI Act does not include a definition of "foundation models" but of "general-purpose AI models" in Article 2(63):
'general-purpose AI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;.
The seminal report on foundation models proposes a definition based on two key features: i). they are trained on broad data; and ii). they can be adapted to a wide range of downstream tasks. Rishi Bommasani et al. *On the Opportunities and Risks of Foundation Models.* 2022. arXiv: 2108.07258 [cs.LG].

Second, the transactional component (actions and decisions directed to pre-contractual, contractual and post-contractual purposes). The general notion of 'contracting' is intended to cover not only the contract formation stage but any preceding or posterior stage related to a contract or to an envisaged contract. Therefore, this Paper refers to digital assistants searching and selecting best offers for consumers, recommender systems, algorithmic negotiation or renegotiation, AI systems concluding contracts, automated performance of contractual obligations and/or enforcement of agreed consequences in case of default. Thus, algorithmic contracting encompasses pre-contractual actions, contract formation, and a variety of performance-related situations, including termination and enforcement of agreed consequences for default.

The decision to use this term is aligned with the ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts.[15] And it has been employed to define the scope of the ADM-readiness test of the European Union consumer protection acquis conducted as a first result of the Project.[16]

As explained above, the notion of automated system includes deterministic algorithmic models that operate according to instructions and models with AI techniques that incorporate learning capabilities and operate according to (pre-determined or even evolving) objectives. This distinction is particularly relevant for the analysis of vulnerability risks and the assessment exercise on the adequacy of existing legal rules and principles to algorithmic contracts. The most intense impact on the classical elements of private law proves to be particularly exerted by the second category of systems (learning systems). The incorporation of AI techniques provides the distinguishing feature that has, in fact, triggered global concern about its social and ethical implications and has attracted the attention of regulators and legislators worldwide. AI has aroused fear and surprise, scepticism

15 ELI *Guiding Principles and Model Rules on Algorithmic Contracts,* https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/.

16 ELI*, Interim Report, EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* adopted by the ELI Council on 27 November 2023. The drafters of the report and co-rapporteurs of the project are Christoph Busch, Teresa Rodríguez de las Heras Ballell, Dariusz Szostek until October 2023, Christian Twigg-Flesner and Marie Jull Sørensen. Available at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.

and mistrust, fervour and fascination in equal measure. Responses and reactions to and from AI have taken many different forms and formats but share the sentiment of urgency in understanding the risks and the challenges.[17] All of them naturally shape the climate in which legal questions about the use of AI in and for decision-making are addressed.

The formulation of a definition of AI systems for legal purposes faces a number of challenges. It must be free from technological determinants and maintain sufficient (technological) neutrality to encompass the various solutions available (or to come) on the market and to avoid obsolescence by being able to integrate future technological developments. It must translate into functionally and normatively relevant features, operational characteristics and technical specifications. The evolution of the definition of an IA system in the deliberations for an European AI Act[18] highlights these difficulties. The first definition proposed in the AI Act[19] immediately raised several questions and aroused some criticism. Firstly, it failed to convincingly and decisively delineate the proposed AI systems to be regulated from the already commonly used and widely known computer programs

17 OECD AI Principles, https://oecd.ai/en/ai-principles; Policy paper *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023*. Published 1 November 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023; (European Union) High Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI,* 2019 - https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai -; (United States of America), *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* 30 October 2023 - https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

18 Since the first Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules in the field of artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union, COM/2021/206 final, to the finally adopted AI Act. Throughout the process, the definition has evolved in the successive versions – special reference is made to the version of the text dated 14 July 2023. P9_TA (2023)0236 *Artificial Intelligence Act - Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).

19 The proposed AI Regulation (Art. 3(1)) defined the IA system as
"software that is developed using one or more of the techniques and strategies listed in Annex I and that can, for a given set of human-defined objectives, generate output information such as content, predictions, recommendations or decisions that influence the environments with which it interacts".

(software). The regulatory requirements imposed by the new text required a clear and objective distinction as to their scope of application. Secondly, the reference to certain techniques listed in an Annex, despite the establishment of a review mechanism, questioned (in addition to the uniqueness of the chosen techniques themselves)[20] the technological neutrality, the adaptive capacity to new solutions and the very soundness of a purely descriptive definition incapable of offering a functional concept.

The proposed definition has evolved[21] aligning itself with the OECD notion[22] which, following a subsequent revision,[23] strengthens some of the differential functional features and qualifies others[24] in order to accom-

20 Proposed AI Regulation, Annex I, Artificial Intelligence Techniques referred to in Article 3, point 1:
"Machine learning strategies, including supervised, unsupervised and reinforcement learning, employing a wide variety of methods, including deep learning. Logic and knowledge-based strategies, especially knowledge representation, inductive (logic) programming, knowledge bases, inference and deduction engines, expert and (symbolic) reasoning systems. Statistical strategies, Bayesian estimation, search methods and optimization."

21 The latest version of the text, after the compromise agreement reached was made available on 24 January 2024 and includes the following definition: *An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.* In the previous version of the text dated 14 July 2023. P9_TA(2023)0236 *Artificial Intelligence Act - Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD))1 defines an "AI system" as *a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.*

22 OECD, AI terms & concepts, https://oecd.ai/en/ai-principles. OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, May 2029.

23 OECD, AI terms & concepts https://oecd.ai/en/ai-principles, OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, Revision 8 November 2023:
An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

24 As explained in OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, November 2023.

modate the most recent developments that had burst onto the international scene and media debate (large language models, generative AI, general AI). For the purposes of the AI Act, in order to ensure its coverage in the scope of application and to be able to differentiate, in turn, different regulatory regimes depending on the AI model, in the successive amendments to the proposed IA Act two other definitions were added along with the notion of IA system that were not in the initial version: 'foundation model'[25] and 'general purpose IA system'. Subsequently, in the latest text, these definitions have also changed. Foundation model was finally replaced with 'general-purpose AI model'.

For the purposes of this Paper, the notion of algorithmic contracting starts from the definition of 'AI system' in the European regulation. This is the definition adopted by the final text of the AI Regulation. Four main axes on which the concept of an AI system is based are identifiable: interactivity, adaptivity, autonomy and influence on the environment. AI systems are capable of generating outcomes that influence the environment in which they operate on the basis of a set of objectives, either explicit or implicit, which may have been determined at design[26] or learned later in their operation. These outcomes may consist not only of predictions or recommendations, but also of decisions and content of the most diverse nature. This is widely considered in generative AI models. To generate these

25 In the text published on 24 of January 2024, the definition of 'general purpose AI model' already is:
an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities.
Previously, in the P9_TA(2023)0236 *Artificial Intelligence Act - Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).
Art. 3.1.c) '*foundation model' means an AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks.*
The definition is not included in the latest text after the political agreement in December 2023 and as published in January 2024.

26 RAJI, Inioluwa Deborah, HOROWITZ, Aaron, KUMAR, Elizabeth and SELBST, Andrew, "The fallacy of AI functionality", *FAccT,* 2022, 959.

results, systems use data or information that they receive, infer, perceive from the environment, and learn by means of learning methods.

The axes along which the definition of AI systems has been built and revolves around are particularly relevant to the legal analysis of automated decision-making and, in particular, algorithmic contracts. There are several very significant implications.

First, the ability of AI systems to perform actions, make decisions and generate content has an immediate, substantial and direct impact on the contractual logic. An AI system can accept an offer, elaborate a contracting proposal, execute an action aimed at fulfilling a contractual obligation, or terminate the contract.

Second, the potential of AI systems to (relatively but increasingly) autonomously learn[27] according to varying levels of autonomy challenges settled notions of consent and intent, error, or actually the conception of contract as a meeting of minds. The very rapid advances of generative AI models[28] and the exponential growth of their capabilities are already beginning to raise the possibility that they may derive in 'emergent behaviours'[29] aimed at circumventing human control, optimising resources to achieve the goal in a sub-optimal way, using persuasion techniques or pretending to be human.

Third, adaptive, learning, and evolving capacity injects unpredictability into the outcome and raises questions concerning the treatment of error, the effect of unexpected or surprising learning, the attribution of legal effects or the allocation of liability.

---

27 In this rapidly evolving context, the term 'frontier AI models' has been proposed to define those models with the potential to pose serious risks to public safety and global security. The dangerous capabilities that such AI models would present include even the possibility of circumventing human control through deception and obfuscation. The authors of the paper *Frontier AI regulation: Managing emerging risks to public safety* (2023. arXiv:2307.03718 [cs.CY]) acknowledge that it is not yet clear whether models will tend to develop in this direction, but it is argued that this could be the result of current training paradigms: NGO, Richard,
CHAN, Lawrence and MINDERMANN, Sören, "The alignment problem from a deep learning perspective", 2023. arXiv: 2209.00626 [cs.AI].

28 OECD, *Initial policy considerations for Generative Artificial Intelligence, OECD Artificial Intelligence Papers,* September 2023, num. 1.

29 CHAN, A. et al., "Harms from Increasingly Agentic Algorithmic Systems", IEEE Computer Society, 2023, Vol. 2022-March, 2023, https://arxiv.org/abs/2302.10329.

From these defining and differential axes of AI systems, the legal problems of automated contracts emerge, and the legal issues that we are going to analyse are built on them.

From this definition, we can now delineate with full precision the scope and meaning of the notion of algorithmic contracting. Automated contracting comprises the use of AI systems at one or more stages of the life cycle of a contract, by one, several or all parties to a transaction.

Under this broad term, several algorithmic contracting scenarios will be described below with the ultimate aim of assessing the impact on decision-making and gauging the potential vulnerability risks involved therein.

II. Mapping algorithmic contracting scenarios

Firstly, automated systems can be used to exclusively assist a decision or an action finally taken or executed by a natural person or to directly execute the action or take the decision from which the relevant legal effects are to be derived. In the first case, the system selects, compares and recommends the most suitable providers according to certain parameters to facilitate the party's selection and final decision process. In the second scenario, the system repeatedly and automatically, without human intervention in each of the actions, assesses the suppliers, reviews the conditions and continuously concludes supply contracts to optimise the value chain. The legal issues are more numerous and substantial in the second scenario.

Secondly, automated systems can be used exclusively by one of the parties or by several or all the parties involved. Considering the negotiation, conclusion or performance of a bilateral contract, the unilateral use of an ADM system by only one of the parties will raise issues arising from human-machine interaction such as the need to disclose that an ADM system is used, the actual freedom to decide whether or not to contract with or restrict the use of automated systems, the ability of the system to process all information generated in the interaction (the requirement for terms and conditions to be in an accessible and machine-readable format)[30] or, for example, the risk of manipulation of the ADM system. The dual (or

30 Article 14 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act, hereinafter DSA), OJEU No. 277, 27 October 2022. DUCATO, Rossana and STROWEL, Alain, 'Limitations to text and data mining and consumer empowerment: making a case for a right to machine

multilateral, if relevant) use of ADM systems leads to an environment of pure and full interaction between 'machines' (M2M, *Machine-to-Machine*) where in addition to all the general issues (validity, attribution, liability, pre-contractual information) it could suggest new ones such as the effects on the contract of interoperability restrictions, the reconsideration of the notion of balance or imbalance in the negotiating position of the parties or, if the parties use a common platform for their interaction, the risk of conflicts of interest or the intervention of the platform operator as an intermediary (mediator, service provider, representative, agent).

ADM systems can be used in consumer relations, either by the consumer (virtual assistants,[31] *chatbots*, digital assistants)[32] or by the trader, or by both parties. The impact of the use of ADM systems in consumer relations,[33] especially when it is the consumer who uses them, goes beyond mere questions of terminology and the applicability of consumer protection legislation to these cases, and may invite a profound and radical rethinking of some of the paradigms that have established the foundations on which consumer law has been built.

---

legibility', *International Review of Intellectual Property and Competition Law,* 2019, vol. 50, num. 6, 649-684.

31 To the extent that a virtual assistant, as defined in the EU regulation, performs an action with contractual effects, e.g. initiating a subscription or executing a contractual obligation or right (such as access to a service). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Regulation). OJEU No. 265 of 12 October 2022 (hereinafter the GDPR).
Art. 2.12). "*Virtual assistant" means software that can process requests, tasks or questions, including those formulated by means of sounds, images, text, gestures or movements and that, on the basis of such requests, tasks or questions, provides access to other services or controls connected physical devices.*

32 Or *intelligent agents* in the sense of Arno R. LODDER and Marten B. VOULON, in "Intelligent Agents and the Information Requirements of the Directives on Distance Selling and E-commerce", *International Review of Law, Computers & Technology,* 2002, vol. 16, 77.

33 SEIN, Karin, "Concluding Consumer Contracts via Smart Assistants: Mission Impossible under European Consumer Law", *Journal of European Consumer and Market Law,* vol. 7, 2018, 179; BUSCH, Christoph, "Does the Amazon Dash Button Violate EU Consumer Law? Balancing Consumer Protection and Technological Innovation in the Internet of Things", *Journal of European Consumer and Market Law,* 2018, vol. 7, 80.

On the one hand, the *acquis communautaire* on consumer protection seems to respond to the use of automated systems (*ADM-readiness test*)[34] with consistency and, upon implementing certain improvements and modifications, it seems to maintain robustness and effectiveness. However, this conclusion of reasonable adequacy does not necessarily imply that 'no action' is the optimal strategy or the one that guarantees resilience and sustainability in the future. For, in fact, on the other hand, far-reaching movements are transpiring in the conception of the underlying asymmetry in the consumer relationship that may require rethinking some of the paradigms of consumer law. While the intensive use of AI seems to aggravate the exposure to vulnerability risks, making vulnerability (digital vulnerability)[35] almost endemic in the digital environment, it heralds, on the other hand, an empowerment of the consumer that strengthens their bargaining position and would seem to question the value and ultimate function of classic protection measures such as information rights. It may be argued that an 'augmented consumer', assisted by automated systems in making much more 'informed' decisions, is emerging. This is a critical turning point where risks and vulnerabilities are magnified, while at the same time, the asymmetry of the bargaining process might be substantially reduced and some of the classic protective responses to consumer relations might start losing, in this context, their meaning and purpose, at least to a certain extent.

Thirdly, in automated (or algorithmic) contracting, a distinction has to be made between the contract in relation to which the AI system is used in one of the contractual steps and the peripheral contracts necessary for the use of such an ADM system for the negotiating purpose. Contracts for the supply of ADM systems, for the design or development of an AI system, for training, for the provision of data or for upgrades necessary to be able to negotiate, conclude or execute an algorithmic contract define the ecosystem

34 This is the main, and provisional, conclusion of the report produced by the team of the *ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts*, after conducting the *ADM-readiness test* on the main consumer rules of the *acquis communautaire*. ELI, *Interim Report*, *EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* adopted by the ELI Council on 27 November 2023. The drafters of the report and co-rapporteurs of the project are Christoph Busch, Teresa Rodríguez de las Heras Ballell, Dariusz Szostek until October 2023, Christian Twigg-Flesner and Marie Jull Sørensen.

35 HELBERGER, N., SAX, M., STRYCHARZ, J., MICKLITZ, H.W., "Choice Architectures in the Digital Economy: Towards a new understanding of digital vulnerability", *Journal of Consumer Policy,* 2022, vol. 45, 175-200.

necessary for algorithmic contracting to take place. The focus is not on these agreements, which may or may not be partially automated, but on the final contract that is negotiated, concluded or executed using AI systems whose availability depends, in effect, on this prior or contemporaneous contractual framework. The contract we are interested in is not the one concluded between the party who wants to use an AI system to negotiate with his suppliers and the developer of such a system, whether standard or customised. However, in the analysis of some of the issues that should be addressed, this interaction and influence may be relevant. Thus, for example, knowing the conditions under which the design and development of the AI system has been commissioned may be a factor in assessing the degree of control of the system by the operator using it in automated contracting, in assessing the existing of an error, or in choosing product liability rules as a response to an unforeseen action of the system causing damage

B. Identifying legal issues of algorithmic contracts and exploring uniform solutions

Electronic contracting, a few decades ago, posed a challenge to legacy contract law.[36] Traditional contract-law rules had been ideated, formulated, and applied, paradigmatically, for face-to-face and in-writing distance transactions highly dependent upon the available medium, dominantly paper, and the means of communications for sending and received relevant declarations and other statements between the parties. The use of telephone or telegram had indeed required, prior to the advent of digital technologies, an explicit legal recognition in civil and commercial codes. Electronic contracting confronted traditional contract law with the admissibility of the digital medium as a functional equivalent to writing in paper and the use of electronic communications[37] to express and convey declarations of

36 UNCITRAL texts in the 1996 Electronic Commerce Model Law (with Guide to Enactment) – hereinafter, MLEC; 2001 Electronic Signatures Model Law (hereinafter, MLES); 2005 Use of Electronic Communications in International Commerce Convention (hereinafter, CEC) approved by General Assembly Resolution 60/21, of 23 November 2005.

37 CEC Article 8. Legal recognition of electronic communications

will and other statements with pre-contractual, contractual or contract-performance relevance. Under the fundamental principles of technology neutrality and functional equivalence, essentially, [38] international instruments and domestic legislation incorporated the necessary provisions to ensure the validity and enforceability of electronic contracts[39] as well as other declarations or actions along the contract life cycle.

Algorithmic contracting, as defined above, goes beyond electronic commerce and pose additional challenges to existing legal rules, even if they are modernized to accommodate electronic contracts. While electronic commerce's challenge stems from the use of electronic communications, algorithmic contracting's one lies in automation.

ADM systems do not simply transmit or enable the transmission of an offer, an acceptance or any other relevant communication between the parties as electronic means do, but, in assisting, or even making decisions, they (automatedly and autonomously, that is the key) produce an output, that may amount to be an offer, an acceptance, or a communication of contractual modification.[40] The difference is substantial and enormous. The simple problem of attribution that electronic communications, once their

---

"1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.
(…)"
"Electronic communication" is defined as "any communication that the parties make by means of data messages; while "data message" is defined as "information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy".

38 Mainly, as formulated in MLEC, MLES, and CEC.

39 Article 12 CEC seems to go further than the pure electronic contracts and explicitly acknowledges:
"A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract."

40 As an illustration in the EU *acquis*, Article 9 of the Directive on Electronic Commerce (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) OJ L 178, 17.7.2000, 1–16) does not refer to contracts concluded by automated means, but simply to contracts concluded by electronic means:
Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic

validity and enforceability had been recognised, posed, and was effectively solved, is exacerbated by automation. If ADM systems repeatedly and automatedly (even more intensively if autonomously) produce outputs, without human intervention in each and every action and decision, the question of to whom to attribute such decisions and their resultant legal effects is of paramount importance. The answer is neither evident nor necessarily easy. As automation includes not only deterministic algorithmic decision-making but also AI-driven learning systems, the attribution of legal effects and the allocation of risk in case of mistakes, damages or harmful consequences gain complexity and significance. To the automated self-execution, it has to be added the assumption of certain levels of autonomy in the decision-making and the performance.

Therefore, it has to be discussed whether existing legal rules on electronic contracts are suited to algorithmic contracting on an extended functional-equivalence approach, or, on the contrary, there are novel challenges that algorithmic contracting poses.

Algorithmic contracts tense the most classical features of the notion of a contract as a meeting of minds. Unlike electronic contracts that simply transform how declarations of wills are manifested, stored, and transmitted, algorithmic contracting touches the human-centric core of contract law. Although humans are not certainly excluded from the scene, as they participate in designing or deploying the system, they may express their consent in using such automated mechanisms for a particular purpose (or the consent might be inferred from the fact of deploying and using), or they (can) select the criteria on which the system operates, or the data sources feeding the ADM system, the distinctive features of ADM precisely lie in the decision-making capabilities of the system and its operation "without human intervention" in each and every action carried out thereby.

Therefore, the validity and enforceability of contracts concluded by ADM as well as of any action performed in connection with any stage of the contract life cycle (pre-contractual, contractual, performance, termination) need to be assured.

---

contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.
The current wording acknowledges two fundamental principles: first, that contracts can be validly negotiated and concluded by electronic communications: declarations (data messages) in digital form and transmitted by electronic means; and secondly, that contracts can be validly concluded in a digital medium.

I. A rule of legal recognition

A strong case is made to unambiguously harmonized a rule of legal recognition.[41] Such a rule must recognize that the validity and enforceability of a contract should not be denied on the sole ground that it is was formed by automated systems. This rule entails that other grounds could challenge the validity or the enforceability of the contract though ("on the sole ground that"). The fact that automated systems have, without human intervention, formed the contract is not compromising the validity or enforceability of the contract. Additional rules may be required (and should be indeed formulated) to address other issues that are likely to impact on the validity and enforceability of the contract, such as the state of mind, mistake, or any other defects of consent. Nevertheless, a firm legal recognition as formulated above is instrumental to lay the foundations to establish a sound legal framework for algorithmic contracts. It dissipates any fundamental and radical objection in admitting that they can be legally binding contracts despite the 'human distance' from the processing to reach a meeting of minds.

No distinction, at least in principle, should be drawn between dual situations where both parties are automated systems or non-dual ones if only one of the parties is resorting to an automated system. As far as the legal recognition principle is concerned, there is no solid reason to alter it. However, specific rules or safeguards might be necessary in the second

41 UNCITRAL, A/CN.9/WG.IV/WP.182, 4:
Principle 2. Legal recognition
(a) A contract is not to be denied validity or enforceability on the sole ground that an automated system was used in its formation.
(b) An action in connection with the formation of a contract is not to be denied validity or enforceability on the sole ground that it was carried out by an automated system.
(c) An action in connection with the performance of a contract is not to be denied validity or enforceability on the sole ground that it was carried out by an automated system.
In the final version of the MLAC (A/CN.9/LVII/CRP.9), the rule of legal recognition is laid down in Article 5:
Article 5. Legal recognition of automated contracting
1. A contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in any action carried out in connection with the formation of the contract.1
2. An action carried out by an automated system in connection with the formation or performance of a contract shall not be denied legal effect, validity or enforceability on the sole ground that no natural person reviewed or intervened in the action.

scenario if a special vulnerability arising from human-machine interaction is assumed and expected to be mitigated.

The rule of legal recognition is to be extended over any action in connection with the contract and throughout the entire contract life cycle. Thus, it includes actions carried out by the automated system during the precontractual stage (automated negotiations), a unilateral proposal to renegotiate a formed contract, actions to perform by one or both parties any of the contractual obligations, an action to exercise a right to withdrawal, or a prior notice for termination.

The term 'action' is intendedly neutral and aims to encompass all kinds of outcomes an automated system may generate. These outcomes, in the context of a commercial transaction, range from mere mechanical actions activated by the instruction sent by the ADM system to the interconnected device, to content generated by the system and addressed to a variety of recipients (humans or devices) – data, code, digital content, digital service – to be processed. Hence, the outcome can consist of an instruction sent by the ADM system to a delivery robot to process a purchase order, a specific data to be integrated in the contract (an update of the rent or the price fixed as per the pricing mechanism), or a draft document (an offer, a draft contract, a legal brief, a notification as per the contract, a termination letter) or any other content (voice, visual art, music or code). As foundation models and generative-AI tools are gaining overwhelming scale and growing sophistication, generative capabilities have to be properly acknowledged and sufficiently embraced by any terminology employed to describe which actions are carried out by automated systems.

The choice of a perfect term to embrace all these types of outcomes automated systems are capable of generating is not easy.[42] 'Actions' seem a viable solution to the extent that cover equally a variety of outcomes that may have legal effects and, therefore, will be subject to a proper legal categorization in each case. The idea of using explicitly the term 'decisions' to classify certain outputs generated by automated system raise concerns about an attempt to attribute legal capacity and personify automated systems. To avoid such a misconception, it seems more reasonable to keep the notion neutral and address the attribution issue with an attribution rule, as discussed below.

42 UNCITRAL, A/CN.9/1132, para. 65(b)) Deliberations of the Working Group IV on this matter (see A/CN.9/1125, paras. 28, 69, 77 and 86; A/CN.9/1093, para. 56).

II. Attribution rules

The legal recognition rule leads to a fundamental discussion on attribution of the legal effects. Having discarded any attempt to grant personhood or recognise automated systems as distinct and separate persons, an attribution mechanism is essential. Promoting algorithmic contracting in and for commercial activities depends upon a predictable and sound enabling legal framework providing clear rules for attribution of legal effects, and allocation of risks.

Several features of algorithmic contracting explain why attribution may be uncertain.

First, AI system can operate with 'varying levels of autonomy'. Assuming certain levels of autonomy and learning capabilities of the AI system questions a perfect, deterministic predictability of the output and, therefore, challenges a simple attribution model. How to face unexpected outputs from the perspective of contract rules?

Second, various actors are involved in the design, the training, the deployment, and the operation of an ADM system. Hence, it can be discussed whether the outputs are decisively, majorly, or partially determined by the design, by the completeness and adequacy of the training process, by the quality and the quantity of data, by the decision to use that system for a particular purpose, or by the lack of an update. All these elements can influence on the final output, but it has to be decided to whom to attribute the output and its legal effects. This question is not referring to the allocation of risks and, therefore, it is not diving into the liability rules. The attribution question is simple, but essential. Whose actions are carried out by the system? Should the output generated by the ADM system turn out to be an offer, who is the offeror; should the system accept an offer and the contract is concluded, who are the contracting parties; should the system omit relevant information in the negotiations, who might be held liable for infringing the pre-contractual duty to inform; should the system send a notice of termination, whether the contracting party is duly exercising their right to terminate with prior notice.

Third, complexity, opacity, data-dependency or openness characterizing AI systems may obscure a full and total comprehension of the process leading to the output to be attributed, even by the person who uses the system for a particular purpose. A company who relies on an automated-negotiating solution may feel that the preliminary dealings are developing in an uncontrolled or unexpected manner, or simple that they are inexplicable.

These features characterising AI-driven decision-making lead to two undesired risks.

On the one hand, uncertainties on the attribution of the outputs and their legal effects. Contracting would be highly discouraged, if parties are uncertain about who is engaged in the negotiations and who is the counterparty. Such an ambiguity is simply an unacceptable risk for the commercial activity. It would be unexpected for a negotiating party to realize that the binding offer produced by an automated negotiating system is surprisingly attributed to the programmer of the automated system, unknow by the party and unconnected to the negotiations, a data provider, an update provider or any other actors involved in the design, the deployment of the training of the automated system. That is an absurd and surprising result. It has to be prevented with the formulation of a clear attribution rule. In the dim notion of vulnerability that was used at the beginning, it can be argued that the characteristics of AI may create situations of asymmetries, imbalances, and uncertainties throughout the contract lifecycle that require a proper adjustment. To that extent, it was suggested that vulnerability can also be combatted with the formulation of (harmonized) basic contract rules aimed at clarifying attribution, ensuring predictability in the allocation of risks, or providing clear rules on error, unexpected outputs, or malfunctioning.

On the other hand, parties might opportunistically allege such features of AI system (complexity, opacity, vulnerability, data-dependence or openness) as an excuse not to assume the consequences of such actions or not to comply with their obligations. Parties engaged in algorithmic contracting might be tempted to avoid their obligations on the grounds that the relevant actions were carried out by automated systems. This risk would destroy legal certainty in trade and definitively ruin the prosperity of algorithmic contracting. In the same vein, not addressing this opportunistic risk with adequate rules would stoke forms of vulnerability on the counterparties.

A simplified attribution rule that states that the actions of a system shall be attributed to 'the person on whose behalf the system is operated'[43] has several serious limitations.

First, it is only providing a solution when that person on whose behalf the system is operating can be identified. The difficult cases are where such a link is not explicit or evident and cannot be inferred from the circumstances. Two illustrations can help to distinguish such cases. If the

43 UNCITRAL, A/CN.9/WG.IV/WP.182, Principle 4.

chatbot engaged in the negotiations is embedded in a digital environment (website, platform, app) visibly controlled and managed by a company (the trader), these circumstances lead to presume that the chatbot's actions are attributed to that company. If the parties agree to use automated systems to fix certain criteria for the performance of their contractual obligations, such an explicit identification is sufficient and conclusive. Complications arise from cases where neither the parties state, nor the practices between the parties or the surrounding circumstances reveal such an assumption.

Second, the relationship between the ADM system and the person to whom to attribute its actions is not and should not be treated as an agency relationship. The automated system is not 'acting on behalf of' in pure terms ('the person on whose behalf the system operates'), as that might re-open the debate on the personhood of AI systems. Should the wording 'on whose behalf the system is operated' is, however, simply referring to the fact that the system is operated (by a third party) on behalf of the principal (to whom to attribute), this is not more than a traditional rule of attribution between persons (agent and principle). If it is formulated so, there is no mystery. The real conundrum is to whom to attribute the actions of 'the' system as such.

Third, the attribution rule should not only provide a predictable and objective model for third parties interacting with the automated system to rely on, but also for the person to whom the actions are to be attributed. Such an attribution should not be unexpected, unreasonable or surprising when based on or dependent upon inadequate factors to presume attribution. In this regard, the mere use, as a pure factual factor, might be inadequate. Some illustrations may explain better the inadequacy. A bank decides to use a chatbot to handle complaints from its customers, and unexpectedly the chatbot renegotiates the loan conditions. An industrial company uses robots in its smart warehouse, and in one of the updates entirely conducted and controlled by the manufacturer, a smart functionality is installed in the robots that become to make purchase orders on an automated basis. A new office building is equipped with sophisticated smart devices and systems collecting data from staff performing and a business rent the office space without predetermining which data will feed the systems and on which criteria operate, but the automated gates start banning the entry to employees classified, by the system, as 'unreliable'.

Considering the unwanted effects of the 'use' as the single factor for attribution, two other elements can be considered: control and purpose.

The (natural or legal) person who decides to use an automated system for contractual purposes is expected to adopt measures to keep it under certain control: commissioning the design of the system under a set of instructions, customizing a standard system provided in the market by a developer, fine-tuning a general-purpose model, ensuring that it is fit-for-purpose, seeing to timely maintenance or update, or deploying a proportionate human supervision. It cannot be ignored that the concept of control is elusive and complex, and maybe it should be labelled differently to avoid confusion with the notion of 'control' enshrined in other UNCITRAL instruments (notably but not exclusively, the Model Law on Electronic Transferable Records, MLETR)[44]. Specially, control potentiality seems to contradict the characteristics inherent to AI systems (opacity, complexity, autonomy, openness). Nevertheless, the idea of control is still the most convincing to bridge the attribution link, albeit embedded in other elements. The control factor is not aimed to be used as a limitation or an excuse for a party to assume its actions in a contractual context, by proving lack of control; on the contrary, the notion of control intends to find a reasonable solution where parties are silent, as well as to provide incentives for the parties using automated systems to adopt proper measures to effectively take control.

In the final text, the MLAC tackles the attribution problem with a two-layer rule (Art. 7 MLAC). First, in concordance with primary B2B scope, parties' autonomy. Paragraph 1 states: 'As between the parties to a contract, an action carried out by an automated system is attributed in accordance with a procedure agreed to by the parties'. Second, a combination of 'use' and 'purpose'. Thus, if paragraph 1 does not apply, 'an action carried out by an automated system is attributed to the person who uses the system for that purpose'.

The presumption of attribution by a qualified use (not a passive use but an active use based on the capacity of influencing to some extent on determining performance criteria) would also apply to a consumer who uses an ADM system in or for contracting purposes (digital assistant). In this case, however, additional safeguards might be required. In the ELI Project on Algorithmic Contracts, several solutions have been proposed.[45]

---

44 UNCITRAL Model Law on Electronic Transferable Records, 2017, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records.

45 ELI, *Interim Report, EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* adopted by the ELI Council on 27 November 2023. The drafters of the report and co-rapporteurs of the project are Christoph

First, that the 'control' by the consumer in the terms and to the extent set out below should be configured as a design parameter (*control by design*).

Second, that ADM systems for offering virtual assistant services to consumers that allow automating any of their stages of the contract life cycle should be classified as high-risk systems, in the classification of the AI Act.

Third, that consumer's 'control' should be understood to exist only if the following three requirements are satisfied: a). the ability to approve or object to a contract agreed through a digital assistant prior to its conclusion; b). the ability to set (and review) the parameters that a digital assistant uses to make its decisions; c). the right to suspend or disconnect a digital assistant. In the latter case, the exact scope of this right could depend on the types of business models, or monetisation strategies, that may emerge in relation to digital assistants, in particular where these are an integrated feature of physical products (*smart products*).

The approach adopted by the ELI Project invites two deeper reflections.

On the one hand, if and to which extent the attribution phase and the selected attribution factors (may) constitute a potential source of digital vulnerability in consumer transactions. Should the attribution factors fail to effectively and properly articulate the actual consent of the consumer and convey in an equivalent way an informed decision, the consumer is exposed to new forms of vulnerability. Then, it should be asked whether a specific action is needed to alleviate such a risk.

On the other hand, if the attribution solution formulated as a harmonized rule in the UNCITRAL work has not been, in principle, guided by any vulnerability concern, whether the same attribution factors can and should work in a different scenario intersected by the perception of higher vulnerability risks. The question is fascinating as it leads to a profound and radical discussion on policy options. Should attribution be indeed a common issue, regardless of the condition of the parties, the rule and the factors should remain intact. How then to protect vulnerable parties at this stage? One option is to accommodate the attribution rule or the attribution factors in order to prevent vulnerability scenarios. That raises the delicate issue of the reasons to differentiate basic contract-law rules depending on the condition of the parties, or maybe the circumstances of the transaction (environment, means, interfaces). The latter one addresses an interesting structural perspective of the digital vulnerability – linked to and stemming

Busch, Teresa Rodríguez de las Heras Ballell, Dariusz Szostek until October 2023, Christian Twigg-Flesner and Marie Jull Sørensen.

from the environment itself. Another option is not to alter the basic rule of attribution, but to work on defining specific and more adequate control criteria, together with other safeguards (right to object), to prove relevant control for attribution purposes.

The discussion above bridges the formulation of harmonized rules for the use of AI/ADM systems for contracting purposes with the debate on digital vulnerability in the context (consumer) algorithmic contracting.

C. Decoding digital vulnerability in algorithmic contracting: a two-sided interplay

A digital-vulnerability approach to algorithmic contracting leads, at least in an initial phase, to consequently advocate for the preservation of the paradigms and the backbone principles of consumer protection legislation. That would result from three main principles: the principle of attribution, the principle of application of consumer rules, and the principle of non-alteration of the duty to provide information. As per the principle of attribution, the starting point is that the actions and decisions of the virtual assistant are 'of the consumer'. That is, properly coupled with design measures that ensure that the consumer has and retains control, the actions of the ADM system are considered by the law as actions attributable to the consumer. Thus, the status of the parties (consumer-trader) is not altered by the use of ADM systems. The immediate and natural consequence is therefore the principle of application of consumer law, as the conditions for its application would not have changed in any way. In particular, the information obligations, which channel the paradigm of transparency in the consumer market, should not be reduced or altered despite the intervention of virtual assistants.

With the above three principles, algorithmic contracting in consumer relations is based on the logic and principles of consumer protection law. Notwithstanding this at least provisional conclusion, the opportunity should not be missed to reopen certain debates and to question some of the solutions embedded in the current conception of consumer law. It is an old debate that warns that information obligations are, on the one hand, a burden[46] for the trader, heavier as smaller is the size, and, on the other

46 BEN-SHAHAR, Omri and SCHNEIDER, Carl E., *More than you wanted to know: The failure of mandated disclosure. Princeton,* NJ: Princeton University Press, 2014;

hand, that they are very often (at least to some extent) inefficient[47] and do not produce the expected result. The information model has obvious limits that blur its effectiveness. Limitations in information processing or comprehension, short attention spans, lack of reading, imperfect rationality, cognitive biases and prejudices, education and experience, are factors that inevitably impact on the foundations of the model.[48] Flooding the market with information does not lead to the myth of perfect transparency, nor does it necessarily lead the normative consumer model to make rational, pro-consumer decisions. While information obligations continue to increase in legislation and, in particular in relation to AI systems, continue to play a protective role, there is a call for a transformation of information duties,[49] an adaptation of the form, channels and characteristics of the message to ensure its readability, comprehensibility, appropriateness and adequacy, personalisation and contextualisation. Digital assistants and other AI systems could be designed to meet these expectations by improving the comprehensibility, contextualisation and sufficiency of information, adjusting its tone and personalising the content, completing, verifying or expanding where necessary for each consumer and each transaction. But, we may ask ourselves, does this make the consumer more powerful or does

GARCIA PORRAS, Catherine and VAN BOOM, Willem, "Information disclosure in the EU Consumer Credit Directive: Opportunities and limitations", in J. DEVENNEY and M. KENNY (eds.), *Consumer credit, debt, and investment in Europe*, Cambridge, UK: Cambridge University Press, 21-55; MAROTTA-WURGLER, Florencia, "Will increased disclosure help? Evaluating the recommendations of the ALI's 'principles of the law of software contracts", *University of Chicago Law Review*, num. 78, 2011, 165-186; MAROTTA-WURGLER, Florence, "Does contract disclosure matter?", *Journal of Institutional and Theoretical Economics*, num. 168, 2012, 94-119.

47 SEIZOV, Ognyan, WULF, Alexander J. and LUZAK, Joanna Aleksandra, "The Transparent Trap. Analyzing Transparency in Information Obligations from a Multidisciplinary Empirical Perspective", *Journal of Consumer Policy*, num. 42, issue 1, 2019, 149-173.

48 BAR-GILL, Oren, "Consumer Transactions" in ZAMIR, Eyal and TEICHMAN, Doron (eds.), *The Oxford Handbook on Behavioural Economics and the Law,* Oxford: OUP, 2014, 465-490. AYRES, Ian, and SCHWARTZ, Alan, "The No-Reading Problem in Consumer Contract Law", *Stanford Law Review*, 2015, vol. 661, 545-610.

49 PICHONNAZ, Pascal, "Informed Consumer or Informed Parties: Towards a General Information Duty?", *European Journal of Consumer Law/ Revue européenne de droit de la consommation* (EJCL/REDC) 2023/2, *Is consumer law obsolete?*, 267-281; PICHONNAZ, Pascal, "The transformation of information duties", in TWIGG-FLESNER, Christian and MICKLITZ, Hans (eds.), *The Transformation of Consumer Law and Policy in Europe,* Oxford/London: Hart/Bloomsbury, 2023.

it make him responsible for his own protection? Does it make sense to shift the burden of the information duty from the trader to the consumer assisted by AI systems? What effects would this shift have on the market in general and on the liability of traders in particular?

The starting point here should be then the opposite: the use of ADM systems for consumer decision-making can strengthen the consumer's position and improve bargaining power. If a consumer, assisted by a digital assistant, i.e. by an AI system that searches and processes information, selects and recommends options or even makes the final contracting decision with a prior review of the purchase conditions, is in a position to make better informed decisions, the use of ADM systems in consumer relations accompanies and makes the protective function of consumer law more effective. If such a premise is assumed, the limitation or prohibition of their use will be avoided or prevented as far as possible because it empowers the consumer. The underlying debate is much more complex, with more nuanced premises and less forceful conclusions, but at this point we only take one of the argumentative threads to address the question of the conventional prohibition of the use of automated systems, in particular by the consumer. In short, whether the principle of non-discrimination of ADM systems in contracting, reinforced by the premise that it also mitigates the consumer's vulnerabilities and improves his bargaining position, is transformed into a right of use without limitations or barriers in consumer relations. Interestingly, this idea shifts the spotlight from the assumption that ADM systems generate new forms of vulnerability to the enticing presumption that a consumer deprived of the assistance use of ADM is rendered more vulnerable. Accordingly, vulnerability faces must be also attacked by ensuring fair access and equal use to those systems likely to reinforce the consumer position in contracting.

Without going into the body of the study, which deserves due attention elsewhere, we dwell on one of the principles proposed in the ELI (*European Law Institute*) project on algorithmic contracting.[50] Of the eight principles

50 Details of the ongoing *ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts can be* found at https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/. The report approved by the ELI Council on 27 November 2023 and published in the same year, *Interim Report, EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM,* examines the adequacy of existing rules while already anticipating some of the principles that will guide the second phase of the project aimed at formulating a set of principles and model rules for automated contracting.

tentatively proposed in the first phase of the project, principle 4 (*Non-discrimination and 'no-barrier' principle*) encapsulates the idea that consumers can benefit from the use of ADM systems for trading and contracting. Moreover, ADM systems in the form of digital or virtual assistants can most effectively and fully realise the ultimate ratio of the 'informed decision'[51] which the consumer makes with full knowledge and full, adequate and sufficient information to ensure that it is in his or her best interests. Both in their current state of development and in their expected future evolution, ADM systems operating as digital or virtual assistants for consumers would act as powerful managers of transaction-relevant information. They can collect, contrast, compare and verify information provided by traders about the product, recommend the best combination of attributes, advise on the most appropriate contractual terms, negotiate certain terms, search for the best offer, reject proposals incorporating contractual terms that the consumer has marked as unacceptable, or dynamically review long-term relationships such as subscriptions or contracts for the supply of products or services. These functionalities and potential applications of digital assistants would seem to dilute the weakened position of a consumer unable to deal with scattered, overwhelming, biased or complex information. The digital assistant stands as a consumer protection wall and a 'manager of consumer interests' with unparalleled collection, verification, integration and search capabilities.

On a first reading, algorithmic contracting would seem to rebalance consumer relations, eliminating asymmetries and reducing the need for safeguards. But the context is much broader and more complex and cannot, and should not, be solved with the erroneous assumption that there are no more 'consumer relations'. Indeed, as a starting point, the ELI project on algorithmic contracting starts from the principle (*Principle 2: Application of Consumer Law to Algorithmic Contracts*) that the actions of the virtual assistant are attributed to the consumer and, as such, we are dealing with consumer relations to which consumer protection rules apply. Perhaps this should only be an interim and transitory answer that will have to be discarded when (if) the transition to M2M transactions in all economic

51 Article 2(e), Directive 2005/29/EC of the European Parliament and of the Council 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*), OJEU L 149/22, 11.6.2005.

operations is completed. Then, we will have to refocus intervention on 'technological asymmetries' and 'digital vulnerabilities'.

Nor are we here analysing the intricate question of the attribution of information from the virtual assistant to the consumer and its possible impact on the content and scope of the information obligations of the trader.

Therefore, we are only assessing whether, given the effect of the strengthening of the consumer's position that the use of automated systems seems to have, the limitation or prohibition of their use by the employer would be appropriate. The principle of non-discrimination and *non-barrier* has two derivatives. On the one hand, the prohibition of a differentiated and unfavourable treatment of consumers who use automated systems compared to consumers who do not. On the other hand, the prohibition that the entrepreneur prevents the use of virtual assistants for contracting. But in neither of its two variables is the principle absolute. In fact, the debate on whether a genuine 'right to use' ADM systems should be recommended and crystallized into duties on the trader not to prevent, limit or restrict has been complex and remains open. Competing interests are pitted against each other and do not facilitate a one-colour solution.

The effective exercise of an eventual right to use ADM systems for contracting by consumers would require, first, preventing the use of technological, operational or design measures that block, deter or disable the use of virtual assistants (*blockers*); and, second, implementing contractual, technological and design solutions that facilitate the virtual assistant to perform the necessary actions under equivalent conditions. Digital spaces (websites, applications and other digital user interfaces) should be designed in such a way that they do not pose a barrier to automated systems or, moreover, that they are *ADM-friendly, i.*e. suitable for use by digital assistants. For example, a digital assistant must be able to allow a digital assistant to 'use' a withdrawal button on a website (and the digital assistant must have this functionality). Another important element which is already expressly provided for in the regulation and which will be key for virtual assistants to play their role is that the information to be provided by traders must be available in machine-readable form and, of course and cumulatively, in a form which is intelligible to the consumer (Art. 14 RSD)[52]. This is the

52 Article 14(1) DSA, General conditions:
'Intermediary service providers shall include in their general terms and conditions information about any restrictions they impose in relation to the use of their service

only way to avoid *de facto* discrimination against consumers assisted by automated contracting systems.

The implementation of these technological and operational, design and programming measures involves costs and requires changes in communication channels, interfaces and contracting procedures. They could therefore become a burden for small companies, putting them at a disadvantage vis-à-vis established market players and large platforms. This disruptive effect on the market has to be taken into account in the final shaping of the principle of non-discrimination and *non-barrier*. But in addition, and from another perspective that applies equally to small and large entities, the use of automated systems can saturate the system, simultaneously block available offers without completing the transaction, alter prices or erroneously generate messages of non-availability (*bots* for purchasing tickets or tickets, assistants that keep multiple transactions pending simultaneously, *bots* that saturate the system and block it, automated systems that multiply bookings). The above examples illustrate that there may be cases where legal restrictions (and valid contractual prohibitions) may exist or be imposed on the use of AI systems to protect specific interests, such that their use becomes unlawful, inappropriate or unreasonable.

D. Rethinking paradigms to address digital vulnerability: towards a notion of algorithmic or ADM-related vulnerability

The use of ADM in and for contracting alters the a/symmetries between the parties, re-allocates the risks throughout the contract life-cycle, and dynamically re-balances the power relationships in the transactional context. As a consequence, algorithmic contracting invites the revisit of legacy paradigms and principles underpinning the classical notion of vulnerability. Concurrently, the use of ADM in transactional contexts aggravates certain vulnerabilities, and creates new ones, whereas it proves to mitigate or eliminate other vulnerability factors.

---

in respect of information provided by recipients of the service. This information shall include details of any policies, procedures, measures and tools used to moderate content, including algorithmic decision-making and human review, as well as the procedural rules of their internal complaint handling system. It shall be in clear, plain, intelligible, user-friendly and unambiguous language, and shall be made publicly available in an easily accessible and machine-readable format'.

Therefore, the interplay between algorithmic contracting and digital vulnerability is complex, multifaceted, and challenging. It goes beyond the concept of digital vulnerability. In fact, considering the source of the potential vulnerabilities, exploring a concept of algorithmic (or ADM-related) vulnerability would be promising and advisable. This 'algorithmic vulnerability' stacks on the notion of digital vulnerability. It builds on it but it adds a new layer of challenges. Algorithmic vulnerability naturally resides in the context where digital vulnerability emerges.

The notion of algorithmic vulnerability would acknowledge the impact of the use of ADM in the framework of the digital architecture and in digital relations. However, its challenges are distinct and lead to different vulnerability scenarios.

The vulnerability assessment needs to solve first the main legal issues arising from the use of ADM/AI system for contractual purposes. As expounded in this Paper, at least two rules are absolutely critical in laying the foundations for a legal framework enabling algorithmic contracting: legal recognition rule and attribution rule. A strong case for international uniform rules has been made. And the adoption of the MLAC by UNCITRAL responds to it with an articulated solution.

Only then, it can be explored the algorithmic contracting territory through the lens of vulnerability concerns. And the image displayed is complex, paradoxical, and still blurry. The use of ADM systems for contractual purposes leads to new forms of inequality and vulnerability risks as well as offers promising possibilities to re-equilibrate balances and repair failures that would mitigate the perceived vulnerabilities. The interplay between digital vulnerability and algorithmic contracting is two-sided. And a narrower notion of 'algorithmic (or ADM-related) vulnerability' emerges and should be more closely studied.

Digital Vulnerability of Consumers in the World of Smart Contracts – Is European Private International Law "Digitalised" Enough?

Jura Golub

A. Introduction

This contribution deals with consumer smart contracts in the context of European Private International Law (EU PIL). The concept of smart contracts is not new and has its roots in the 1990s, but it has regained prominence with the development of blockchain technology in the context of cryptocurrencies.[1] Although blockchain is not a necessary precondition for smart contracts, as the concept can also function through other electronic means, this contribution will focus on smart contracts based on blockchain technology.[2] In the simplest terms, smart contracts can be defined as computer programs based on code that contain predefined obligations that are automatically performed. This represents a significant difference compared to traditional contracts written in natural language.[3] Smart contracts operate based on conditional logic rules. The algorithm's operation is programmed with "if" and "then" conditions, meaning that when a previously established condition is met, the smart contract automatically performs a predefined action that has also been programmed in advance.[4] Automation, as a characteristic of smart contracts, in a legal sense, eliminates the need

1 Mateja Đurović, "What are smart contracts? An attempt at demystification" in Zvonimir Slakoper and Ivan Tot (eds), *Digital technologies and the law of obligations* (Routledge 2022), 123.

2 Antonio Davola and Roberto Pardolesi, "What is Wrong in the Debate about Smart Contracts" (2020) 9(5) Journal of European Consumer and Market Law 201, 205.

3 Florian Möslein, "Smart contracts and civil law challenges: Does legal origins theory apply?" in ByIris Chiu and Gudula Deipenbrock (eds), *Routledge Handbook of Financial Technology and Law* (Routledge 2021), 30; Mateja Đurović and Chris Willett, "A legal framework for using smart contracts in consumer contracts: Machines as servants, not masters" [2023] MLR 1, 5-6.

4 Olaf Meyer, "Stopping the Unstoppable: Termination and Unwinding of Smart Contracts" (2020) 9(1) Journal of European Consumer and Market Law 17, 17-18.

for trust between parties. Transactions are conducted automatically and autonomously without the possibility of unilateral changes or manipulation.[5] Furthermore, as an additional benefit of smart contracts, lower transaction execution costs can be mentioned because smart contracts eliminate the need for intermediaries, such as courts or lawyers, as the performance of obligations is automated.[6]

However, it is important to mention certain risks associated with smart contracts. It is possible that the automatic execution of a smart contract does not correspond to previous agreements between the contracting parties made outside the blockchain. Also, due to the rigidity of contract automation, parties may be unable to modify the terms in the smart contract later due to changed circumstances.[7] Given the automation above as a critical characteristic of smart contracts, there is inevitably a digital vulnerability for consumers arising from the likely lack of understanding of new technological concepts for the majority of consumers due to the imbalance in technological and legal knowledge, as well as the economic power between consumers and professionals in the digital marketplace.[8]

While there are numerous substantive discussions about whether smart contracts are legally binding agreements in contract law, this contribution will focus on issues related to European Private International Law (EU PIL) without assessing the validity or invalidity of smart contracts in terms of contract law. Therefore, the main research question in this paper is whether EU PIL provides an adequate legal framework in the context of international jurisdiction and conflict of laws rules for smart consumer contracts. This leads to the following sub-questions: Do the obligations defined and/or performed by smart contracts fall within the scope of EU PIL instruments for contractual relationships? Can the contracting parties in a smart contract define a choice of court or law clause, and in the absence or invalidity of such a choice, which court is competent or which law applies to smart consumer contracts?

---

5 Maren K. Woebbeking, "The Impact of Smart Contracts on Traditional Concepts of Contract Law" (2019) 10(1) JIPITEC 106, 107.

6 Saša Nikšić, "Očitovanje volje i suvremene informacijske tehnologije" in Marko Baretić and Saša Nikšić (eds), *Zbornik treće regionalne konferencije o obveznom pravu* (Pravni fakultet Sveučilišta u Zagrebu 2022), 44.

7 Oscar Borgogno, "Usefulness and Dangers of Smart Contracts in Consumer Transactions" in Larry A DiMatteo *et al* (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (CUP 2019), 292-293.

8 BEUC, *EU consumer protection 2.0: Structural asymmetries in digital consumer markets* (Joint report, 2021), 5.

In light of the above, this contribution sets two research objectives. First, it is essential to determine whether disputes arising from "smart contractual relationships" exhibit the characteristics of "civil and commercial matters" within the meaning of the Brussels Ibis Regulation[9], and whether such relationships entail contractual obligations within the scope of the Rome I Regulation[10]. Furthermore, if it can be considered that smart contracts fall within the scope of the aforementioned EU PIL regulations, it is necessary to establish whether smart contracts, as a digital phenomenon, fit into the existing framework of EU PIL concerning the application of specific rules for determining international jurisdiction and the applicable law in business-to-consumer transactions (B2C). Since smart contracts are based on blockchain technology, which enables transactions between people worldwide, questions of the localisation of legal relationships are of utmost importance for private international law.

In this contribution, an overview of the characteristics of blockchain technology and the concept of smart contracts based on it will first be briefly presented. Subsequently, the characterisation of smart contracts in the context of EU PIL will be carried out in terms of international jurisdiction and conflict-of-law protection for consumers as the weaker party. Finally, the conclusion will address the previously posed research questions.

B. Setting the scene of smart contracts

As previously stated, this contribution addresses legal issues related to smart contracts based on blockchain technology in the context of EU PIL. However, before further analysing the characteristics of smart contracts, it is advisable to begin by explaining the features of blockchain technology as the technological foundation of smart contracts.

Blockchain technology is based on Distributed Ledger Technology (DLT), a broader concept consisting of interconnected computers or nodes. These nodes function to identify users and verify transactions cryptograph-

9 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L 351 (Brussels Ibis Regulation).

10 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations [2008] OJ L 177 (Rome I Regulation).

ically.[11] The EU has provided a normative definition of DLT through several legal acts. In EU law, DLT is defined as a technology that enables the operation and use of a data repository that records transaction data. This data repository is distributed among a network of nodes and is synchronised among these nodes through a consensus mechanism.[12] DLT is an encrypted database containing a ledger to record participant transactions.[13] The purpose of DLT is to facilitate the sharing and updating of information in a distributed and decentralised manner. This involves interconnected computers functioning as nodes, which can be geographically located anywhere in the world.[14] This poses new challenges for private international law. One of the key characteristics of DLT is the absence of a central authority or intermediary that oversees or manages the system. Instead, this role is carried out by the networked computers or nodes, highlighting the decentralisation of the database.[15]

Building upon the previous discussion regarding DLT, blockchain technology is subsequently introduced, and it has gained broader attention due to the emergence of cryptocurrencies. The blockchain protocol consists of interconnected computers or nodes that cryptographically identify participants and verify their transactions before recording them in the system. Participants in blockchain transactions are identified using cryptographic keys. These keys include a public key that serves as a publicly visible ad-

11 Jura Golub, "Characterisation of Cryptoassets as a Separate Category of Digital Assets" in Ivana Kunda *et al* (eds), *Balkan Yearbook of European and International Law 2022* (Springer 2023) 196-197.

12 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU [2022] OJ L 151, arts 2(1) and 2(2); Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L 150, arts 3(1)(1) and 3(1)(2).

13 Francisco J. Garcimartin Alferez and Sara Sanchez, "Is private international law tech-proof? Conflict of laws and FinTech: selected issues" in Thomas John *et al* (eds), *The Elgar Companion to the Hague Conference on Private International Law* (Edward Elgar Publishing 2020) 407.

14 Robin Hui Huang, *Fintech Regulation in China: Principles, Policies and Practices* (CUP 2021), 98; Kelvin F. K. Low and Eliza Mik, "Pause the Blockchain Legal Revolution" (2020) 69(1) International and Comparative Law Quarterly 135, 137.

15 Low and Mik (n 14) 137.

dress and a private key, a password known only to the specific participant.[16] Each blockchain node manages a full copy of the verified transactions in the blockchain ledger. Packets containing recorded transaction data are referred to as blocks. Each block is linked to the next block using cryptographic signatures, creating a chain. This feature enables the blockchain to function as a ledger that can be accessed with appropriate permissions. Since all transactions are recorded in all nodes, transactions always leave an immutable trace, and data cannot be altered, as is the case when data is stored only by a central intermediary.[17]

Finally, it is necessary to highlight the differentiation of blockchain manifestations. The fundamental division of blockchain is into public and private forms. In a public blockchain, anyone can participate without fulfilling specific prerequisites, and participants are generally of unknown real identity.[18] On the other hand, a private blockchain can only be accessed by specific individuals who meet certain requirements for participation on a particular blockchain platform, and their identity can be determined either by other participants or by a gatekeeper who verifies whether an individual meets the prerequisites for participation in the private blockchain.[19] Furthermore, concerning the permission level, public and private blockchains can be permissionless, where all participants are authorised to execute transactions, or they can be permissioned, where only certain blockchain participants are authorised to execute transactions.[20]

Building upon the explanation of DLT and blockchain technology, the concept of smart contracts is introduced. Smart contracts, as computer programs that contain programmed contractual obligations and/or instructions for performing obligations in the form of computer code, are recorded on a blockchain network (such as Ethereum) and are automatically executed when a triggering event occurs, without the need for human intervention in performing the obligations.[21]

16 Alferez and Sanchez (n 13) 407.

17 Hague Conference on Private International Law, *Developments Concerning PIL Implications of the Digital Economy* (Prel. Doc. No 4 REV of January 2022) para 14.

18 European Law Institute, *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (Report, 2023), 23.

19 ibid 28.

20 ibid.

21 Law Commission, *Smart legal contracts, Advice to Government* (Law Com No 401, 2021), paras 2.28 - 2.29.

While it is common for smart contracts to be used solely to perform obligations from a contract written in natural language, it is also possible for smart contracts to be used for entering into legally binding contracts.[22] Given this dual functionality, smart contracts can be classified into two categories. The first category consists of smart contracts, where the code of a computer program executes the automated performance of contractual obligations. In this case, the smart contract serves solely as a means of performance obligations defined in an "external" contract, entered into in natural language.[23] Such smart contracts will be called "off-chain" smart contracts in this contribution. On the other hand, there is a type of smart contract in which the contractual terms are defined in the code of a computer program, and the obligations are also automatically performed by the algorithm, but there is no external version of the underlying contract in natural language.[24] Such a smart contract that exists exclusively in the blockchain environment will be referred to in this contribution as an "on-chain" smart contract.

Furthermore, there is an additional third type of smart contract in which the blockchain functions as an autonomous party that enters into a contract with another contracting party without specific human approval and automatically executes it.[25] In this case, it involves an artificial intelligence (AI) agent that accepts an offer or autonomously creates a counteroffer on behalf of its principal.[26] This type of smart contract concluded through an AI agent, is considered particularly suitable for consumer contracts because autonomous generation allows adaptation to individual consumer needs.[27]

Forming a smart contract involves the offeror writing the contract terms in a specific programming language and posting the written contract on a particular blockchain platform as an offer.[28] The offer is followed by another participant's acceptance of the offer on the blockchain, which can

22 Đurović and Willett (n 3) 1.
23 Law Commission (n 21) para 2.51.
24 ibid.
25 Đurović Mateja and Janssen André, "Formation of Smart Contracts under Contract Law" in Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (CUP 2019) 66.
26 Woebbeking (n 5) 110.
27 ibid 110.
28 Andre Janssen , "Smart Contracting And The New Digital Directives: Some Initial Thoughts" (2021) 12 JIPITEC 196, 199.

be manifested by performance (e.g., making a cryptocurrency payment), or the intention to accept the offer can be indicated by approval through a private cryptographic key.[29] When the offer and acceptance are thus combined, the smart contract automatically performs the obligations according to the pre-programmed parameters.

The potential practical applications of smart contracts in consumers' everyday lives are numerous. Examples include smart contracts in car rentals, where the car can be used as long as the fees are paid, and automatic locking prevents further use if the payments are not made. They can also be applied to utility services (gas, electricity, water), where the supply of services continues as long as the obligations to the service provider are met. Additionally, they can be used in supply chains, enabling automatic reordering of groceries as soon as certain items are depleted in the consumer's household.[30]

C. Do smart consumer contracts fall within the framework of EU PIL?

Before further considering the issues of jurisdiction and applicable law in the context of smart contracts, it should be emphasised that only some legal relationships related to smart contracts between a professional and a consumer will necessarily lead to applying EU PIL rules. The fact that a smart contract is based on blockchain technology, with nodes dispersed worldwide, does not automatically mean that the legal relationship has an international element.[31] For a legal relationship to be characterised as international, there must be a subjective or objective element connecting the legal relationship to a specific foreign legal system.[32] In the case of smart contracts, it is possible to have a B2C transaction between a professional and a consumer from the same country, which is not relevant from the perspective of EU PIL. However, considering the characteristics of blockchain

29 Dino Gliha and Sandra Marković, "Smart Contracts and Human Rights" in Zvonimir Slakoper and Ivan Tot (eds), *Digital technologies and the law of obligations* (Routledge 2022), 174.

30 Janssen (n 28) 200.

31 European Law Institute (n 18) 28.

32 Julia Hörnle and Ioannis Revolidis, "Civil and Commercial Cases in the EU: Jurisdiction, Recognition, and Enforcement, Applicable Law—Brussels Regulation, Rome I and II Regulations" in Julia Hörnle (ed), *Internet Jurisdiction Law and Practice* (OUP 2021), 269-270.

technology, it would be opportune to assess each legal relationship related to smart contracts under the presumption that there is an international element.[33] Therefore, in this contribution, further discussions of smart consumer contracts are placed in the context of EU PIL, assuming the existence of an international element.

As a protective category of contracts, the Brussels Ibis Regulation and the Rome I Regulation for consumer contracts establish special rules regarding international jurisdiction and conflict of laws to protect consumers as the weaker party to the contract. The purpose of having specific rules for consumer contracts is to address the vulnerability of consumers due to their specific position in the legal relationship compared to the other contracting party, which is typically a professional. Generally, the weaker party is considered in a subordinate position or exposed to greater vulnerability.[34] From the perspective of EU PIL, consumers are considered particularly vulnerable in a legal relationship due to information asymmetry regarding the content of applicable law and the rules for determining the competent court. They also face social and economic subordination in relation to the professional.[35] In addition to protecting consumers as the weaker contracting party, these special rules on jurisdiction and conflict of laws aim to ensure predictability in legal relationships.[36]

The Brussels Ibis Regulation is applied for determining jurisdiction and the recognition and enforcement of judicial decisions in civil and commercial matters, except for those matters that are explicitly excluded from the scope of application of this Regulation. Its counterpart, the Rome I Regulation, is applied in cases of conflict of laws regarding contractual obligations in civil and commercial matters, and its application is also excluded in certain matters.[37] Therefore, regarding smart consumer contracts, the following questions arise: Do the obligations defined and/or performed by automated smart contracts fall within the concept of "civil and commercial

33 Luís de Lima Pinheiro, "Laws Applicableto International Smart Contractsand Decentralized Autonomous Organizations (DAOs)" (2023) 3(1) International Journal of Cryptocurrency Research 16, 20.

34 Ilaria Pretelli, "A focus on platform users as weaker parties" in Andrea Bonomi *et al* (eds), *Volume XXII Yearbook of Private International Law – 2020/2021* (Verlag Dr. Otto Schmidt 2021), 214.

35 Giesela Rühl, "The Protection of Weaker Parties in the Private International Law of the European Union: A Portrait of Inconsistency and Conceptual Truancy" (2014) 10(3) Journal of Private International Law 335, 343-345.

36 Geert van Calster, *European Private International Law* (Hart Publishing 2013), 134.

37 Brussels Ibis Regulation, art 1; Rome I Regulation, art 1(1)(2).

matters," and can they be considered "contractual obligations" within EU PIL?

At the outset, it is essential to emphasise that the terms contained in the corpus of EU PIL for contractual obligations have an autonomous meaning. They must be interpreted independently of national concepts to ensure uniform application across all Member States, irrespective of their national law.[38] Given that this contribution aims to examine aspects of international jurisdiction and conflict-of-law protection for consumers in the context of smart contracts, relevant provisions of the Brussels Ibis Regulation and the Rome I Regulation, although serving different purposes, are interpreted as connected to achieve consistency.[39]

The concept of "civil and commercial matters" should be understood broadly, covering all principal civil and commercial matters. This is achieved by distinguishing between public and private law.[40] The decisive criterion for distinguishing them is the exercise of public power, meaning the ability of one of the parties in a legal relationship to exercise public power, which is otherwise not permitted to private persons.[41] This demarcation can also be applied to relationships related to smart contracts, whether they are concluded off-chain or on-chain. The parties' legal positions will be assessed in these relationships, determining whether one party exercises public power over the other. If that is the case, such a legal relationship does not fall under the scope of EU PIL instruments for contractual relationships.

According to the Court of Justice of the European Union (CJEU), the concept of "contractual obligations," or as Article 17(1) of Regulation Brussels Ibis states for consumer contracts, "matters relating to a contract," should be understood to encompass all legal relationships in which one contractual party voluntarily assumes an obligation towards another party.[42] It is important to note that, for the application of Regulations Brussels Ibis and Rome I, a contract is not even necessary to be concluded. These regulations apply in any situation where it is possible to identify

38 Case C-419/11 *Česká spořitelna, a.s. v Gerald Feichter* [2013] ECLI:EU:C:2013:165, para 45.

39 Rome I Regulation, recital 7.

40 Martin Illmer *et al*, "Scope and Definitions" in Andrew Dickinson and Eva Lein (eds), *The Brussels I Regulation Recast* (OUP 2015), 61-62.

41 Hörnle and Revolidis (n 32) 269.

42 Case C-26/91 *Jakob Handte & Co. GmbH v Traitements Mécano-chimiques des Surfaces SA* [1992] ECR 1992 I-03967, para 15.

the existence of a specific obligation, except if such an obligation falls within the scope of specific matters that are excluded from the application of Regulation Brussels Ibis or Rome I.[43] Furthermore, the mutuality of obligations is irrelevant when defining the concept of a "contract" under EU PIL. The term "contract" and the scope of EU PIL instruments equally cover unilateral and bilateral legal transactions.[44]

If we consider the way on-chain smart contracts are formed, it is evident that even in the case of such a digital phenomenon, there is an act of freely assuming obligations, whether unilateral or bilateral. The offeror places the contract terms on the blockchain platform, while on the other side, the offeree expresses willingness to enter into the contract either by using a private cryptographic key or simply performing the obligations.[45] Therefore, there is a voluntary assumption of obligations, and accordingly, on-chain contracts fall within the scope of the application of the EU PIL for contractual obligations. However, this still does not mean that such contracts are valid. Every contract, including a smart contract, will be legally binding only if the legal effect is recognised by the applicable law to which the conflict of laws rules refer.[46]

In assessing the character of obligations arising from off-chain smart contracts as "contractual obligations," there should not be significant obstacles, considering that the obligation is accepted outside the blockchain system in natural language. In such cases, the nature of the obligation as a "contractual obligation" is assessed as with any other traditional contract, and the automatic performance of the obligation through a smart contract is just one aspect of the external underlying contract.

After defining the concepts of "civil and commercial matters" and "contractual obligations," it is necessary to consider the criteria of the relevant EU PIL regulations regarding characterising a specific contract as a consumer contract.

43 Case C-419/11 *Česká spořitelna, a.s. v Gerald Feichter* [2013] ECLI:EU:C:2013:165, para 46.

44 Case C-180/06 *Renate Ilsinger v Martina Dreschersa* [2009] ECR 2009 I-03961, para 51.

45 Đurović and Janssen (n 25) 67-68.

46 Florence Guillaume, "Aspects of private international law related to blockchain transactions" in Daniel Kraus *et al* (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar Publishing 2019), 68; Rome I Regulation, arts 10(1) and 11(4)(5).

Regulations Brussels Ibis and Rome I define legal relationships that similarly fall within the scope of protective rules for consumer contracts concerning jurisdiction and applicable law. According to the relevant Regulations, consumer contracts are defined as contracts concluded by a consumer as a natural person for a purpose outside his/her trade or profession with another contracting party acting within his trade or profession, i.e., with a professional under one of the following conditions: 1) the professional conducts his commercial or professional activities in the state where the consumer has his/her habitual residence/domicile, or 2) the professional directs such activities to that state or several states by any means, including that state, and the contract falls within the scope of those activities.[47] Additionally, Regulation Brussels Ibis extends the protective jurisdiction for consumer contracts to include contracts for the sale of goods with deferred payment of the price and contracts for credit sales or any other form of credit agreements concluded to finance the sale of goods, provided that the consumer has concluded such contracts for non-professional purposes.[48]

From those above, the following characteristics of a consumer can be summarised. The concept of a "consumer" is objective and entirely irrelevant to the subjective characteristics of a specific natural person regarding his/her specific knowledge and information.[49] Therefore, the characteristic of a consumer is examined solely in terms of the individual's position in a specific contractual relationship, taking into account the nature and purpose of such a legal relationship, where the consumer must enter into the contract for non-professional purposes to satisfy individual needs.[50] In the context of smart contracts, the specific technological, legal, or other knowledge of the consumer is irrelevant as long as such a contractual relationship meets the objective criteria for qualifying a particular contract as a consumer contract.

Regarding the nature of on-chain contracts and the possibility of concluding the external underlying contract at a distance, even in the case of off-chain contracts, the question arises from the professional's perspective of recognising that the other party is acting on the market as a consumer. In this case, everything is in the eyes of the professional, as protective con-

47 Brussels Ibis Regulation, art 17(1)(c); Rome I Regulation, art 6(1).
48 Brussels Ibis Regulation, art 17(1)(a)(b).
49 Case C- 774/19 *A. B. and B. B. v Personal Exchange International Limited* [2020] ECLI:EU:C:2020:1015, para 38.
50 ibid, para 39.

sumer provisions will not apply to a natural person who would generally meet the consumer criteria if such a person, through his/her behaviour with the professional, has given the impression of acting for business purposes, and the professional could not reasonably have known about the private purpose of the delivery.[51] The CJEU has provided several useful indicators to identify such a situation, such as ordering goods that can be used for business purposes, using business equipment, delivering to a business address, or mentioning the possibility of a VAT refund.[52]

However, what raises certain questions are the localisation conditions for the professional's activities, especially the second criterion related to directing commercial activities. In contrast to the first alternative condition, which requires that the professional carries out commercial or professional activities in the country/state where the consumer has his/her habitual residence or domicile, there will generally be no difficulty in recognising such a circumstance. This situation applies when the professional is present in the country/Member State where the consumer has his/her habitual residence or domicile and receives orders from consumers in that area.[53] This is confirmed by German case law. In a specific case, a branch of a French bank in Germany rented a battery for charging an electric vehicle to a German consumer, and the general terms of the contract contained a provision allowing the professional to disable further battery charging in case of contract termination remotely. In this case, the courts characterised the legal relationship as a consumer contract, invoking Article 6 of the Rome I Regulation and Article 18 of the Brussels Ibis Regulation, which established the jurisdiction of the German court and the application of German law as the applicable law. The court also noted that it is entirely irrelevant whether the remote disabling of battery charging is a consequence of automatic blockchain action or the action of an employee.[54]

As mentioned, the situation is somewhat less clear regarding the second alternative condition, which consists of the professional "directing his commercial or professional activities by any means" to the country/Member

51 Case C-464/01 *Johann Gruber v Bay Wa AG* [2005] ECLI:EU:C:2005:32, paras 51 and 53.

52 ibid, para 52.

53 Michael Wilderspin, "Article 6: Consumer contracts" in: Ulrich Magnus and Peter Mankowski (eds), *Rome I Regulation - Commentary* (Verlag Dr. Otto Schmidt 2017), 474.

54 Bundesgerichtshof, Urteil vom 26. Oktober 2022 - XII ZR 89/21, para 14.; OLG Düsseldorf, Urteil vom 7. Oktober 2021 - 20 U 116/20, para 40.

State where the consumer has his/her habitual residence or domicile, or to several countries/Member States, including the country/Member State of the consumer's habitual residence or domicile. Directing activities should be understood as the professional's intention to do business with consumers in the country/Member State where the consumer has his/her habitual residence or domicile.[55] However, in the context of digitalisation and global accessibility of various communication and marketing channels, it is essential to emphasise that the mere availability of the professional's or his intermediary's website in the country/Member State where the consumer has his/her habitual residence or domicile does not necessarily mean that the professional's activity is genuinely directed at that country.[56] In the case of websites, if the professional's activity is presented on his website or that of his intermediary before concluding a contract with the consumer, and it is evident from such websites and the overall activity of the professional that he planned to do business with consumers who have their habitual residence or domicile in one or more countries/Member States, including the consumer's country/Member State, within the context of his intention to conclude contracts with them, the activity will still be deemed to be directed towards the country/Member State of the consumer.[57] In this regard, the CJEU has developed a set of indicative criteria to determine whether the professional directs his activity toward the country/Member State where the consumer has his/her habitual residence or domicile. As indicators of directing activity, among other things, the CJEU mentions the following: the international nature of the activity; the use of a language or currency not generally used in the country where the professional is established; the provision of telephone numbers with international codes; expenditure on internet referencing services to facilitate consumers from other countries access to the professional's or his intermediary's website; the use of a top-level domain name that is not the name of the country where the trader has his establishment; and mentioning an international clientele consisting of customers from different countries.[58] These indicators should be understood as non-exhaustive, and in assessing whether the professional directs his activity, it will be necessary to consider all relevant facts and

55 Pretelli (n 34) 226.

56 Joined Cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG* (C-585/08), and *Hotel Alpenhof GesmbH v Oliver Heller* (C-144/09) [2010] ECLI:EU:C:2010:740, para 94.

57 ibid, para 92.

58 ibid, para 83.

circumstances leading to the formation of a particular smart contract on a case-by-case basis.

It is possible to assume that there may be more challenges in characterising a legal relationship in the case of on-chain contracts based on public blockchains due to their widespread accessibility and the potential for transactions in the realm of anonymity, which complicates the overall evaluation of the case. On the other hand, in the case of on-chain smart contracts based on private blockchains, there should be fewer significant difficulties. This is because there are prerequisites that participants must meet, and the presence of a gatekeeper who verifies the performance of assumptions can provide more clarity and oversight in such cases.

D. International jurisdiction for disputes related to smart consumer contracts

The Brussels Ibis Regulation for consumer contracts prescribes special jurisdiction rules to protect consumers, who are considered the weaker party in contractual relationships, from a procedural and legal standpoint. However, when it comes to smart contracts based on blockchain technology, there is a significant obstacle to legal protection at the outset of the "smart contractual relationship." This particularly applies to public blockchain systems where the true identities of participants are unknown.[59] According to the national rules of civil procedure of EU Member States, a lawsuit must contain details about the defendant, including his name or legal entity name and address.[60] Consequently, if the identities of the contracting parties are unknown, and hence the passive legal standing can not be established, a court will not be able to determine its jurisdiction and, subsequently, apply conflict of law rules to determine the applicable law for smart consumer contracts. In the following discussion, matters of international jurisdiction for legal relationships related to smart consumer contracts will

59 European Law Institute (n 18) 23.

60 German Code of Civil Procedure as promulgated on 5 December 2005 (Bundesgesetzblatt (BGBl., Federal Law Gazette) I page 3202; 2006 I page 431; 2007 I page 1781), last amended by Article 1 of the Act dated 10 October 2013 (Federal Law Gazette I page 3786) and Book 10 last amended by Article 1 of the Act of 5 October 2021 (Federal Law Gazette I, p. 4607), arts 130 and 253; Croatian Civil Procedure Act, Official Gazette No 4/77, 36/77, 6/80, 36/80, 43/82, 69/82, 58/84, 74/87, 57/89, 20/90, 27/90, 35/91, 53/91, 91/92, 58/93, 112/99, 88/01, 117/03, 88/05, 02/07, 84/08, 96/08, 123/08, 57/11, 148/11, 25/13, 89/14, 70/19, 80/22, 114/22, arts 106 and 109.

be examined under the assumption that the identities of the contracting parties are known.

By the jurisdiction rules for consumer contracts, including smart contracts meeting the criteria to be characterised as consumer contracts, the rules are more favourable for the consumer than the professional party. In this regard, a consumer is entitled to initiate proceedings against a professional before the court of the Member State in which the professional is domiciled[61], or alternatively before the court for the place where the consumer is domiciled.[62] On the other hand, a professional is only allowed to bring legal proceedings against a consumer before the courts of the Member State where the consumer is domiciled.[63] In the context of blockchain-based smart contracts and the potential to engage in transactions with professionals across the world, from the perspective of a European consumer, it is important to note that consumers are further protected. Even if the professional does not have a domicile or branch within the EU, the consumer always has the option to initiate legal proceedings before the court for the place where the consumer is domiciled.[64]

Furthermore, Regulation Brussels Ibis allows parties, through mutual consent, to designate the competent court. However, the possibility of choosing a competent court is still significantly limited. The choice of court is only allowed in the following cases: if the choice of court agreement is concluded after the dispute has arisen; if it enables the consumer to bring proceedings before a court other than the courts that would usually have jurisdiction for consumer contracts; or if the agreement is concluded between a consumer and another contracting party, both of whom, at the time of the conclusion of the contract, have their domicile or habitual residence in the same Member State and by which jurisdiction is transferred to the courts of that Member State.[65]

---

61 According to Articles 62 and 63 of the Brussels Ibis Regulation, the court applies its internal law (*lex fori*) when determining whether a party is domiciled in the Member State where the proceedings have been initiated. If the party does not have domicile in the Member State where the proceedings have been initiated, then, to determine whether the party is domiciled in another Member State, the court applies the law of that Member State. Legal persons are domiciled, where they have their statutory seat, central administration, or principal place of business.

62 Brussels Ibis Regulation, art 18(1).

63 Brussels Ibis Regulation, art 18(2).

64 Andrea Bonomi, "Jurisdiction over Consumer Contracts" in Andrew Dickinson and Eva Lein (eds), *The Brussels I Regulation Recast* (OUP 2015), 232.

65 Brussels Ibis Regulation, art 19.

At first glance, it could be more questionable how often choice of court agreements will be concluded in practice in the context of smart consumer contracts due to the limitations above. After a dispute arises, it is highly unlikely that parties, in the form of on-chain contracts, will conclude a choice of court agreement, which would then incur additional costs related to the developer who would need to write the jurisdictional clause into computer code. Additionally, it is uncertain how willing professionals are to agree to such arrangements, enabling consumers to file a lawsuit against them before a court other than the one that would have jurisdiction under protective rules. However, this does not mean that it is not worth analysing whether there is a possibility for the jurisdictional clause to be incorporated into a smart contract. Regarding off-chain smart contracts, there are no obstacles to including a choice of court provision in the underlying contract or in a separate agreement in natural language, provided the prerequisites laid out in the Brussels Ibis Regulation are met. However, the more challenging question is whether a choice of court agreement expressed solely in computer code, i.e., in an on-chain smart contract, can be considered valid.

Exclusively from a technological standpoint of smart contracts, incorporating a jurisdiction clause into an on-chain contract in the form of code is feasible.[66] This can be achieved using programming languages with Turing completeness, meaning they can compute anything.[67] The Brussels Ibis Regulation prescribes several alternative forms of jurisdiction agreements, while in this contribution, particular emphasis is on written agreements.[68] According to the Brussels Ibis Regulation, any communication through electronic means that enables a lasting record of the agreement is considered equivalent to the written form of the agreement.[69] From this, the Brussels Ibis Regulation holds a favourable view regarding the conclusion of jurisdiction agreements through information and communication technologies. Nevertheless, an open question remains concerning comprehending the meaning of a jurisdiction clause drafted in formal language by an average consumer. The CJEU takes the position that the invalidity of a jurisdiction clause cannot be established because it is not drafted

66 cf by analogy Simeona Kostova, *"Party Autonomy in a Modern Context: A Critical Analysis of its Scope under the Rome I Choice of Law Rules and Some Contemporary Considerations"* (University of Aberdeen, Working Paper Series 1/2023, 2023), 23-24.

67 ibid.

68 Brussels Ibis Regulation, art 25(1)(a).

69 Brussels Ibis Regulation, art 25(2).

in the language generally prescribed by the legal system of the Member State where the court decides on jurisdiction.[70] The Member States are not authorised to arbitrarily stipulate additional formal prerequisites for the validity of a jurisdiction clause about those specified in the Brussels Ibis Regulation. Consequently, a jurisdiction clause can be drafted in any language. Nevertheless, it is presumed that the CJEU had natural rather than formal language in mind at the time of its decision. Furthermore, according to Eurostat statistics on the computer skills of individuals, in 2021, only 5.82% of EU citizens wrote code in a programming language.[71] Although knowledge, skills, and experience in writing code over a specific period need not be entirely correlated, it is reasonable to assume that understanding code, or a formal language, is not a common skill among the average European consumer. However, as previously mentioned, the specific subjective knowledge of consumers is entirely irrelevant in determining a natural person as a consumer and, consequently, applying the EU PIL protective rules for consumer contracts.[72]

Therefore, in the case of on-chain smart contracts, a possible compromise solution might involve including a statement in the form of a non-executable comment in natural language within the code, explaining the meaning of the code and specifying that the code pertains to the jurisdiction clause.[73] However, it remains to be seen how comprehensible and unambiguous such comments within the overall code, even in natural language, would be to the average consumer within the complete context. This is especially relevant regarding the potential unfairness of such a smart contract provision, which will be discussed further in the part of this contribution concerning the choice of law clause.[74] In any case, when concluding jurisdiction agreements through electronic communication, including within on-chain smart contracts, it is essential to provide the consumer with the option to save and print the jurisdiction clause before entering into

70 Case C-150/80 *Elefanten Schuh GmbH v Jacqmain* [1981] ECR 1981-01671, para 27.

71 Eurostat, *"Individuals' level of computer skills (2021 onwards)"* (2023) <https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_cskl_i21__custom_8255155/default/table?lang=en> accessed 10 October 2023.

72 Case C- 774/19 *A. B. and B. B. v Personal Exchange International Limited* [2020] ECLI:EU:C:2020:1015, para 38.

73 cf by analogy Law Commission (n 21) para 3.121.

74 See *infra* ch 5.1.

the contract to ensure a lasting record as evidence.[75] Therefore, until the courts establish a definitive standpoint for legal certainty and eliminate the possibility that the choice of jurisdiction clause could be deemed invalid, it would still be most appropriate to conclude the jurisdiction agreement entirely in the natural language outside the on-chain smart contract.

Continuing from the above, one may question the practical purpose of incorporating a jurisdiction clause into an on-chain contract. The segment of an on-chain smart contract containing a jurisdiction clause in the form of computer code, at least for now, could not be automatically executed because the courts exist outside the blockchain system.[76] In order to achieve judicial protection of the contracting parties in an on-chain consumer contract or to establish the jurisdiction of the chosen court, it will still be necessary to provide the court with a translation of the jurisdiction clause from formal language to natural language if it is composed solely in the form of code.[77] Therefore, the insistence of the contracting parties to include the jurisdiction clause in the on-chain contract as the main agreement may be motivated solely by the desire to incorporate substantive and procedural legal issues related to one legal relationship in one place.

Finally, one exception regarding the jurisdiction clause is worth noting. Hypothetically, if an on-chain consumer contract is void under the applicable law, this will not automatically result in the nullity of the jurisdiction clause contained in the on-chain contract as the main agreement. Based on the separability principle, the jurisdiction clause has a separate legal fate and is independent of the main contract in which it is contained.[78]

75 Case C- 322/14 *Jaouad El Majdoub v CarsOnTheWeb.Deutschland GmbH* [2015] ECLI:EU:C:2015:334, paras 32-36.

76 Georgina Garriga Suau, "Blockchain-based smart contracts and conflict rules for business-to-business operations" (2021) (41) Revista Electrónica de Estudios Internacionales 1, 21.

77 Jason Grant Allen, "Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language" in Jason Allen, and Peter Hunn (eds), *Smart Legal Contracts: Computable Law in Theory and Practice* (OUP 2022), 46.

78 Francisco Garcimartin, "Prorogation of Jurisdiction" in Andrew Dickinson and Eva Lein (eds), *The Brussels I Regulation Recast* (OUP 2015), 305.

E. Applicable law for smart consumer contracts

The rules of the Rome I Regulation on determining the applicable law for consumer contracts incorporate all three fundamental principles of EU PIL for contractual relationships: the principle of party autonomy, the principle of the closest connection, and, *per se*, the principle of protecting the weaker party.[79] The specific normative realisation of these principles will be explained further in this contribution, focusing on the concrete application of conflict of law rules in the context of smart contracts.

At the outset, clarifying a few fundamental concepts would be useful. By the Rome I Regulation, "applicable law" is defined as any law indicated by conflict of law rules, whether it is the law of a Member State or a third country.[80] The provision mentioned above embodies the principle of the universality of the applicable law, which is significant in the context of this contribution because, under certain assumptions, consumer contracts can be subject to the law of a third country. This is related to the subsequent application of substantive law, which may or may not provide consumers with the same level of protection as in EU Member States.[81] However, this will be elaborated on further in this contribution.

When we talk about the applicable law for a contract (*lex cause*), it is important to understand that this applicable law covers all issues related to the main rights and obligations arising from a specific contract, particularly the following: interpretation of the contract; performance; consequences of full or partial breach of obligations, including the assessment of damages; ways to discharge obligations and the prescription and limitation of actions; and the consequences of the nullity of the contract.[82] Given the scope of the applicable law, there is a fundamental distinction in determining the applicable law for on-chain and off-chain smart contracts. In the case of off-chain contracts, the object for determining the applicable law is the external contract concluded in natural language, and the applicable law

79 Davor Adrian Babić and Dora Zgrabljić Rotar, "Mjerodavno pravo za ugovorne odnose" in Tatjana Josipović (ed), *Privatno pravo Europske unije – Posebni dio* (Narodne novine 2022), 220.

80 Rome I Regulation, art 2.

81 Francesca Ragno, "The Law Applicable to Consumer Contracts under the Rome I Regulation" in Franco Ferrari and Stefan Leible (eds), *Rome I Regulation The Law Applicable to Contractual Obligations in Europe* (Sellier. European Law Publishers 2009), 136-137.

82 Rome I Regulation, art 12(1).

determined as such will, *inter alia*, cover issues related to the automated performance of the smart contract.[83] On the other hand, when we discuss the applicable law for on-chain contracts, where there is no external base contract in natural language, and the smart contract is formed and executed on the blockchain, the applicable law is determined concerning such on-chain contracts.

The Rome I Regulation distinguishes between subjective and objective applicable law in determining the applicable law for consumer contracts. Subjective applicable law for consumer contracts is the one the parties have chosen (*lex autonomiae*). However, despite the choice of applicable law, the Rome I Regulation stipulates that such a choice cannot deprive the consumer of the protection provided by mandatory provisions of the law that would have been applicable if no party choice had been made, i.e., the law of the state where the consumer has his/her habitual residence as the objectively applicable law (*lex residentiae habitualis*).[84]

When comparing the protective provisions of the Rome I Regulation for consumer contracts to other protective categories of contracts (such as transport contracts, individual employment contracts, or insurance contracts), it is evident that an escape clause is not provided for in the case of consumer contracts.[85] Typically, within the context of the contractual statute of the EU PIL, an escape clause allows a court to apply the law of another state that it deems to have a closer connection with the specific legal relationship instead of the law indicated by the conflict of laws rules.[86] The exclusion of the escape clause could be due to the European legislator's desire to ensure a stable and predictable connecting factor in the consumer's habitual residence in the context of consumer contracts. In the era of new digital technologies, when it is much easier to conclude consumer contracts with professionals worldwide, the absence of an escape clause contributes to consumer protection by removing potential uncertainty in determining the applicable law. It does so by consistently fixing the law of the state of the consumer's habitual residence as the objective law, which is considered reasonable because the professional typically conducts or directs his

83 Pedro de Miguel Asensio, *Conflict of Laws and the Internet* (Edward Elgar Publishing 2020), 427.

84 Rome I Regulation, art 6(1).

85 cf Rome I Regulation, arts 5, 6, 7 and 8.

86 Mirela Župan, *Načelo najbliže veze u hrvatskom i europskom međunarodnom privatnom ugovornom pravu* (Pravni fakultet u Rijeci 2007), 27.

commercial activities within the state of the consumer's habitual residence, objectively representing the *situs* of that legal relationship. However, in the context of on-chain smart contracts based on a public blockchain, when determining the consumer's habitual residence is indeed impossible; this leaves an open problem, as *Professor Rühl* notes.[87] In this case, the conflict of law rules for consumer contracts becomes entirely dysfunctional. This is because it is impossible to determine the consumer's habitual residence, and consequently, it is impossible to identify the objectively applicable law, which serves as the basic conflict of law rule for consumer contracts. As a result, it will not be possible to compare the chosen law's provisions with the objective law's mandatory provisions, ultimately representing a denial of consumer protection as the weaker party in the contract.

Finally, it is worth noting that specific conflict of law protective rules apply to all types of consumer contracts, except for contracts of carriage and insurance, for which there are also specific protective conflict of law rules. Applying these rules also excludes certain specific contracts.[88]

I. Choice of law *(lex autonomiae)*

Regarding the principle of party autonomy, a significant principle in contemporary private law, the European legislator, through Regulation Rome I, allows parties in consumer contracts to choose the applicable law for their

87 Giesela Rühl, "Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?" in Benedetta Cappiello and Gherardo Carullo (eds), *Blockchain, Law and Governance* (Springer 2020), 175-176.

88 According to the Rome I Regulation, art 6 paras (1) and (2) shall not apply to: a contract for the supply of services where the services are to be supplied to the consumer exclusively in a country other than that in which he has his habitual residence; a contract of carriage other than a contract relating to package travel within the meaning of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours; a contract relating to a *right in rem* in immovable property or a tenancy of immovable property other than a contract relating to the right to use immovable properties on a timeshare basis within the meaning of Directive 94/47/EC; rights and obligations which constitute a financial instrument and rights and obligations constituting the terms and conditions governing the issuance or offer to the public and public take-over bids of transferable securities, and the subscription and redemption of units in collective investment undertakings in so far as these activities do not constitute provision of a financial service; a contract concluded within the type of system falling within the scope of art 4(1)(h) of the Rome I Regulation.

legal relationship.[89] However, certain limitations exist despite the general freedom to choose the applicable law. In order to protect consumers as the weaker party in the contract, Regulation Rome I stipulates that the party's choice of applicable law cannot deprive the consumer of the protection provided by the mandatory provisions of the law that would have been applicable had no choice of law been made, i.e., the law of the country in which the consumer has his/her habitual residence as the objectively applicable law.[90] In resolving disputes arising from consumer contracts, this requirement places an exceptionally complex task before the court. First, the court must determine the objectively applicable law, or the law that would be applicable had no choice of law been made, and accordingly, the mandatory rules from which no deviation is allowed by agreement.[91] Then, in the next step, the court compares the level of protection the consumer enjoys based on those rules with the level of protection provided by the chosen law.[92] If the chosen law offers better protection, it is applied. In the opposite situation, if the mandatory provisions of the objectively applicable law provide the consumer with greater protection, primarily, the mandatory provisions of that law are applied, and then, secondarily, the other provisions of the chosen law, resulting in a kind of "law mix".[93] The preceding becomes especially significant in the case of choosing the law of a third country and the global disparity in the level of consumer protection. Considering the nature of blockchain and the possibility of entering into off-chain and on-chain contracts with professionals worldwide, the principle of universalism from Regulation Rome I allows the application of the law of any country, regardless of whether it is the law of an EU Member State. However, despite the choice of third-country law, European substantive law imposes limitations in favour of the European consumer. According to the Unfair Consumer Contract Directive, Member States are required, in the case of a choice of third-country law, to take measures to prevent the consumers from losing the protection provided to them by this

89 Kunda, I., "Međunarodnoprivatnopravni odnosi", in: Mišćenić, E. (ed.), *Europsko privatno pravo: Posebni dio.*, Školska knjiga, Zagreb, 2021, pp. 523-524.

90 Rome I Regulation, art 6(1)(2).

91 cf by analogy Joined Cases C-152/20 and C-218/20 *DG and EH v SC Gruber Logistics SRL and Sindicatul Lucrătorilor din Transporturi v SC Samidani Trans SRL* [2021] ECLI:EU:C:2021:600, para 27.

92 ibid.

93 Rühl, "The Protection of Weaker Parties in the Private International Law of the European Union: A Portrait of Inconsistency and Conceptual Truancy" (n 35) 352-353.

Directive if the consumer contract is closely connected to an EU Member State. [94] The concrete implementation of this provision is carried out when the consumer has his/her habitual residence in an EU Member State, and the national court is obligated to apply those national rules through which the said Directive is transposed into the legal order of the Member State.[95]

Regarding the actual method of choosing the applicable law, Regulation Rome I allows for an express choice of law and an implied choice, i.e., a choice of law that clearly arises from the contract's terms or the case's circumstances.[96] Taking into account the characteristics of computer code, which aims to be precise and clear to eliminate ambiguity, it is likely that the criterion that an implied choice of law arises from the terms of the contract may not be applicable in the case of on-chain smart contracts.[97] However, this does not mean that the criterion of "circumstances of the case" cannot be met in the context of the choice of law for both types of smart contracts. In the case of off-chain contracts, there is certainly the possibility of an implied choice of law that arises from the terms of the contract, given that the underlying contract in natural language exists outside the blockchain. One of the strongest indications of an implied choice of law is often cited as the choice of a competent court.[98] This is significant because if the jurisdiction clause exists solely in the form of code if such a jurisdiction clause is deemed invalid, it cannot be concluded that the actual intention of the contracting parties was to subject the contract to the law of the country whose court's jurisdiction they invalidly chose. Other indicators of an implied choice of law include references in the contract to a specific law or specific provisions of a legal system and practices developed between the parties.[99] Facts such as the place of contract formation, using a specific language, contracting obligations in a particular currency, or the place of performance are not strong enough indicators to conclude an

94 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95, art 6(2).

95 Case C-455/21 *OZ v Lyoness Europe AG* [2023] ECLI:EU:C:2023:455, para 45.

96 Rome I Regulation, art 3(1).

97 Suau (n 76) 24.

98 Francesco Ragno, "Article 3: Freedom of choice" in Ulrich Magnus and Peter Mankowski (eds), *Rome I Regulation - Commentary* (Verlag Dr. Otto Schmidt 2017), 98.

99 ibid 101-102.

implied choice of law. They should be considered in the context of other indicators.[100]

Unlike the assumptions for the formal validity of a choice of court agreement under Regulation Brussels Ibis, about the form of a choice of law agreement in the context of consumer contracts, Regulation Rome I does not require any specific form.[101] The choice of law agreement for off-chain smart contracts is relatively easy. Such an agreement can always be incorporated into an external base contract drafted in natural language.

However, as with the choice of court agreement, the same question arises about the choice of law, i.e., can parties incorporate a choice of law clause into an on-chain contract? Although there are no requirements regarding the form, an agreement on the choice of law drafted exclusively in code form would be unacceptable from the perspective of EU law. According to the CJEU's standpoint, a choice of law clause may be considered unfair if it has certain specific characteristics inherent in its content or context, thereby creating a significant imbalance between the rights and obligations of the parties.[102] In this sense, a provision that fails to meet the requirements of clarity and intelligibility is especially unfair.[103] According to the CJEU's standpoint, this requirement of transparency concerning the clarity and intelligibility of provisions is much broader than mere formal and grammatical intelligibility; it requires full awareness of consumers since they are the weaker party.[104] Therefore, in the case of on-chain smart contracts, a compromise solution similar to the choice of a court agreement would be to include a comment in natural language within the code that refers to the chosen law.[105] Alternatively, parties could conclude a separate choice of law agreement in natural language outside the on-chain contract, ultimately contributing to greater legal certainty for the contracting parties.

100 ibid 103.

101 Bea Verschraegen, "Article 11: Formal validity" in Ulrich Magnus and Peter Mankowski (eds), *Rome I Regulation - Commentary* (Verlag Dr. Otto Schmidt 2017), 706.

102 Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* [2016] ECLI:EU:C:2016:612, para 67.

103 ibid, para 68.

104 Case C-96/14 *Jean-Claude Van Hove v CNP Assurances SA* [2015] ECLI:EU:C:2015:262, para 40.

105 See *supra* ch 4.

II. The consumer's habitual residence *(lex residentiae habitualis)*

The habitual residence connecting factor implements the second foundational principle of EU PIL for contractual relationships, concretely operationalising the principle of the closest connection by establishing that a B2C transaction is most closely associated with the law of the consumer's habitual residence.[106] The application of the habitual residence connecting factor occurs in cases where there is no party's choice of applicable law or when such a choice is invalid. It also applies when a valid choice of applicable law exists, but the court is still obliged to consider the mandatory rules of the consumer's habitual residence and apply the law that offers the consumer greater protection.[107] Consequently, this conflict-of-law rule serves a dual purpose. It acts as a substitute in cases where no choice of law is made and functions as a control mechanism, ensuring that, when a choice of law exists, the mandatory provisions of the country where the consumer has his/her habitual residence that provide greater consumer protection prevail.

In the context of smart contracts, the question arises concerning the relevance of the timing for determining the consumer's habitual residence. In this regard, the relevant moment for establishing the consumer's habitual residence is at the time of contract formation, and subsequent changes in the consumer's habitual residence are irrelevant.[108] The habitual residence connecting factor will play a decisive role in recognising the legal effects of smart consumer contracts. For general contracts under the Rome I Regulation, which do not fall into the protective categories of contracts, the recommendation is that the parties should always choose a law in favour of a country that recognises the legal effects of smart contracts.[109] However, in the case of consumer contracts, the situation is the opposite. Given the significance of the consumer's habitual residence as an objective connecting factor, which simultaneously provides control for consumer protection about the potentially chosen law, in the context of smart consumer contracts, the parties should first consider the mandatory rules of the country where the consumer has his/her habitual residence before choosing applicable law. Although these rules are designed to protect consumers as

106 Kunda (n 89) 512-513.
107 ibid 537.
108 Rome I Regulation, art 19(3).
109 De Lima Pinheiro (n 33) 24.

the weaker party in contracts, it is possible to assume that the complexity of determining the applicable law and the subsequent consideration of a variety of national contract law rules, depending on the habitual residence of each consumer, may lead to hesitation for some professionals in the broader application of smart contracts in internationally-marked consumer transactions.[110]

III. Consent and material validity of smart consumer contracts

When discussing consent and the substantive validity of smart consumer contracts, it is important to understand these concepts broadly. The applicable law for consent and the substantive validity of contracts covers various issues such as the agreement of the contracting parties, the existence of a valid object of the contract, the presence of *causa*, the effects of contract proposals and acceptance deadlines, questions regarding late acceptance, and the existence and scope of the right to terminate the contract.[111] Determining the applicable law for consent and the substantive validity of on-chain smart and off-chain contracts is crucial because these contracts are essentially concluded at a distance. Legal systems concerning distance contracts provide different rules for determining when a contract is concluded and from which point an acceptance produces legal effects.[112] Moreover, considering the previously explained way of forming on-chain smart contracts by posting an offer in the form of code on the blockchain, this conflict of laws rule is important in the context of assessing the existence of the on-chain smart contract itself, especially regarding questions related to the substantive assumptions of an offer made through electronic communication.[113] According to the Rome I Regulation, the existence and material validity of a contract, or any contract provision, are determined according to the law that would be applicable under the Rome I Regulation if the

110 Rühl, "Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?" (n 87) 175.

111 Suau (n 76) 16; Ilaria Queirolo, "Article 10: Consent and material validity" in Ulrich Magnus and Peter Mankowski (eds), *Rome I Regulation - Commentary* (Verlag Dr. Otto Schmidt 2017), 663.

112 De Miguel Asensio (n 83) 474.

113 Franco Ferrari and Jan A. Bischoff, "Article 10 Consent and material validity" in Franco Ferrari (ed), *Rome I Regulation: Pocket Commentary* (Sellier. European Law Publishers 2015), 359.

contract or its provision were valid.[114] The applicable law is determined by the presumption that the contract is valid to establish the applicable law for that contract. In the subsequent step, based on the identified applicable law, the existence or validity of the contract is assessed.[115] In the specific case of smart consumer contracts, both on-chain and off-chain, the practical application of this conflict of laws rules for consent and material validity will generally lead to applying the law of the consumer's habitual residence as the objective applicable law. This should be applied even if the parties have chosen the applicable law, provided that the mandatory rules of the objective applicable law offer the consumer a higher level of protection regarding the consent assumptions and material validity of the contract.

IV. Formal validity of smart consumer contracts

In EU PIL, formal validity is construed as any external expression by a contractual party by which the party manifests the intention to create legal obligations.[116] Generally, formal validity pertains to rules that mandate a specific form of contracting for certain agreements, such as written form, or even involving public authorities like courts or notaries.[117] However, although such contracts are likely a minority due to the particularities of on-chain smart contracts, careful attention will be required concerning the formal validity rules under the applicable law. Specifically, regarding the formal validity of consumer contracts, the Rome I Regulation stipulates that the applicable law is the law of the state where the consumer has his/her habitual residence.[118] The following fact underscores the significance of the formal validity of consumer contracts for consumer protection. The Rome I Regulation, in the case of contracts concluded at a distance through a range of alternative provisions, promotes the principle *in favorem validitatis*, all to preserve the formal validity of contracts by applying one of the offered alternative connecting factors. Nevertheless, for the formal validity of consumer contracts, the exclusive application of the law of the state where the consumer has his/her habitual residence is prescribed.

114 Rome I Regulation, art 10(1).
115 Queirolo, "Article 10: Consent and material validity" (n 111) 663 and 666.
116 Verschraegen (n 101) 694.
117 ibid.
118 Rome I Regulation, art 11(4).

In light of the preceding, the question arises as to what legal consequences may arise in the event of a discrepancy between the law chosen by the parties for a smart contract (*lex causae*) and the law applicable to the formal validity of the smart contract. For instance, in the case of an on-chain smart contract, the law of State A is chosen by the contractual parties as the applicable law for the main rights and obligations (*lex causae*), while according to Article 11(4) of the Rome I Regulation, the law of State B, where the consumer has his/her habitual residence, is exclusively applicable to the formal validity of the on-chain smart contract. This is important because if national law prescribes formalities for certain types of contracts by means of mandatory rules, deviating from the prescribed form may result in the nullity of the contract in certain legal systems.[119] In the aforementioned hypothetical scenario, the on-chain smart contract could formally be void under the law of country B, while the consequences of any nullity would be assessed according to the chosen law of country A (*lex causae*).[120] Although the possibility of a discrepancy is evident, inappropriate results in applying *lex causae* and the law applicable to the formal validity of the contract should not occur. Since the goal of every legal transaction should be to satisfy the interests of each contracting party in a legally permissible manner, the contractual parties, especially the professional, should carefully consider the mandatory rules of the state of the consumer's habitual residence before forming an on-chain smart contract. This is because rules regarding the form of a contract or formal validity in national laws are closely linked to the mandatory rules of substantive law.[121] The prescribed form of a particular transaction always aims, *inter alia*, to provide a higher level of legal certainty and protection among the parties in terms of proving the existence of a legal relationship. Therefore, when considering the mandatory provisions of the law of the state of the consumer's habitual residence, which must always be taken into account as objective applicable law when providing the consumer with a higher level of protection, the parties will generally be informed about the prescribed formal prerequisites for a specific transaction. Finally, if *lex causae* is not

119 German Civil Code in the version promulgated on 2 January 2002 (Federal Law Gazette [Bundesgesetzblatt] I page 42, 2909; 2003 I page 738), last amended by Article 1 of the Act of 10 August 2021 (Federal Law Gazette I p. 3515), art 125; Croatian Civil Obligations Act, Official Gazette No 35/05, 41/08, 125/11, 78/15, 29/18, 126/21, 114/22, 156/22, art 290(1).

120 Rome I Regulation, art 12(1)(e).

121 Verschraegen (n 101) 705.

the law of the consumer's habitual residence, applying the mandatory rules of the state of the consumer's habitual residence is always guaranteed to the consumer if they provide a higher level of protection regarding the consequences of any nullity of the transaction.

In the context of off-chain smart contracts, a specific smart contract will not be the subject of assessing formal validity; instead, it will be the external underlying contract concluded off the blockchain in natural language. The off-chain smart contract's function is solely the automatic performance of obligations, which falls within the scope of *lex causae*.[122]

According to the common understanding, smart contracts are suitable for any transaction, even for transferring real-world assets, including tangible assets such as movables and immovables.[123] However, although from a technological perspective, smart contracts could support the transfer of real property rights, in the actual implementation of the transaction concerning public authorities, there would likely be difficulties since existing national rules often require a written form and the fulfilment of additional prerequisites for registration in the land registry.[124] Without delving into further substantive considerations, it is necessary to draw attention to one exception. Namely, for the main rights and obligations arising from contracts related to rights *in rem* and lease agreements, the protective conflict of laws rules for consumer contracts do not apply.[125] Therefore, a similar exception is prescribed concerning determining the applicable law for the formal validity of such contracts. In the case of these contracts, formal validity is assessed according to the law of the state where the real property is located (*lex rei sitae*), regardless of whether the legal relationship would otherwise objectively meet the conditions for the existence of a consumer contract.[126]

V. (In)capacity of the consumer

Finally, in the discussion regarding issues related to determining the applicable law, attention should be drawn to the risk arising from how primarily

122 Rome I Regulation, art 12(1).
123 Rühl, "Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?" (n 87) 160.
124 Gliha and Marković (n 29) 173.
125 Rome I Regulation, art 6(4)(c).
126 Rome I Regulation, art 11(5).

on-chain smart contracts are formed, which can also apply to off-chain contracts when the base contract in natural language is concluded at a distance. Public blockchain platforms generally do not verify the legal capacity of participants, so a minor or another legally incapacitated person can open a user account and act as a consumer.[127] The specific risk lies in the fact that, according to the substantive law of certain legal systems, binding a legally incapacitated or limited legal capacity person can result in the nullity of the legal transaction.[128]

In principle, questions of legal and business capacity are excluded from the scope of the Rome I Regulation.[129] However, exceptionally, the Rome I Regulation provides that in the case of contracts concluded by persons in the same country, a natural person who, under the law of that country, would have legal and business capacity may invoke the legal incapacity resulting from the law of another country, only if the other contracting party knew of this incapacity at the time of conclusion of the contract, or did not know due to negligence.[130] Although the scope of this provision is narrowed down by a set of criteria, in the context of on-chain smart contracts, the application of this provision will be almost impossible. Namely, from the first criterion that requires the presence of both contracting parties at the time of the contract conclusion in the same country, it is evident that it is highly unlikely to apply the provision about the contracting parties of on-chain contracts from different countries.[131] A similar situation arises in the case of off-chain contracts concluded at a distance in natural language, while the smart contract performs the obligation. Therefore, the determination of the consumer's legal (in)capacity will be governed by national PIL rules, which usually prescribe that the legal capacity of a natural person is determined by the law of citizenship, the law of residence, or the law of the place where the contract was concluded, or the *lex causae*.[132] The consequences of the

127 Đurović and Janssen (n 25) 71; Law Commission (n 21) para 3.24.

128 German Civil Code in the version promulgated on 2 January 2002 (Federal Law Gazette [Bundesgesetzblatt] I page 42, 2909; 2003 I page 738), last amended by Article 1 of the Act of 10 August 2021 (Federal Law Gazette I p. 3515), arts 104 and 105; Croatian Civil Obligations Act, Official Gazette No 35/05, 41/08, 125/11, 78/15, 29/18, 126/21, 114/22, 156/22, arts 276(3) and 330.

129 Rome I Regulation, art 1(2)(a).

130 Rome I Regulation, art 13.

131 Ilaria Queirolo, "Article 13: Incapacity" in Ulrich Magnus and Peter Mankowski (eds), *Rome I Regulation - Commentary* (Verlag Dr. Otto Schmidt 2017), 746.

132 De Miguel Asensio (n 83) 475.

potential nullity of the contract due to the consumer's legal incapacity will be assessed by the *lex causae*.[133]

F. Concluding remarks

From the previously presented contribution, it is evident that the rules of EU PIL for contractual obligations can adequately respond to technological innovations such as smart contracts. Concerning both fundamental types of smart contracts, it is possible to characterise them in terms of "contractual obligations," or "civil and commercial matters," which is a *conditio sine qua non* for applying EU PIL instruments for contractual obligations. Regarding the applicability of existing rules for determining international jurisdiction and the applicable law for legal relationships related to smart consumer contracts, European consumers are in a favourable position, even when entering into legal relationships with professionals from third countries. This favorability arises from two fundamental aspects. Consumers are always entitled to initiate proceedings against a professional before the court of the place where the consumer has his/her domicile, and the existence of a controlling mechanism, the connecting factor of the consumer's habitual residence in the case of a choice of law, ensures that the consumers are always protected by the mandatory rules of the state where they have their habitual residence unless the chosen law provides a higher level of protection.

In light of the above, for legal certainty and the validity of the legal transaction, it would be advisable for the contracting parties, especially the professional, to thoroughly consider the mandatory rules of objectively applicable law. This is done to prevent the legal transaction from conflicting with the mandatory rules of the law of the state where the consumer has his/her habitual residence. Concerning on-chain smart contracts, particular attention should be paid to the rules of the applicable law for the formal validity of the contract, which is assessed solely according to the law of the state where the consumer has his/her habitual residence.

Finally, looking at the broader context of consumer protection, not only from the perspective of EU PIL, it can be concluded that a significant source of vulnerability for consumers in the realisation of consumer rights lies in smart contracts based on public blockchains, i.e. smart contracts in

133 Rome I Regulation, art 12(1)(e).

which the actual identity of the professional is difficult to ascertain, and in the end, possibly permanently unknown. In such cases, consumers would usually be denied legal protection, as it would be impossible to name a specific professional as the defendant in a potential dispute. Consequently, the court will not be able to apply the applicable law. Therefore, stakeholders in consumer protection and policymakers must raise consumer awareness of two fundamental things. First, every private law relationship, even one conducted through modern technologies such as blockchain, is subject to a certain legal order. Second, by entering into a transaction with a professional of unknown identity, consumers risk being deprived of the useful protection the legal system provides as the weaker contractual party.

Addressing Digital Vulnerability Through Private International Law

Gérardine Goh Escolar[*]

A. Introduction

The token economy has powered the recent growth and mainstreaming of Web3 and its "potential to revolutionize agreements and value exchange",[1] leading to the birth of a novel user-led, user-owned economy. Web3 is defined by various parties as the "Read-Write-Own"[2] internet "owned by its builders and users, and orchestrated with tokens".[3] Forecasts increasingly predict that this Web3 economy is expected to outperform the traditional economy based on legacy institutions in various ways.[4]

The rapid advancement of digital technologies has outstripped any other innovation in history. Ubiquitous connectivity through mobile, internet-connected devices, and low-cost data storage, transfer and computing, have enabled new models for the delivery of services and the leveraging of large stores of data. As the largest user of digital technologies today, the financial sector represents a major driver in the digital transformation of the global economy, and will act as a catalyst in enabling equitable access to capital and finance,[5] a crucial step towards global financial inclusion.

* The author thanks Harry Cheng, Raquel Salinas Peixoto, Laura Molenaar, Philippine Chapot, Camilo Saldías Robles, Lwandle Mlalazi van der Niet and Ashlyn Cheong for their assistance. All opinions and any errors contained herein remain entirely those of the author and do not engage the organisations with which she is affiliated.

1 Shermin Voshmgir, *Token Economy: How the Web3 Reinvents the Internet* (2nd ed, Blockchain Hub Berlin 2020), 2.

2 Eshita, 'Web3: in a nutshell' (2021), https://eshita.mirror.xyz/H5bNIXATsWUv_QbbEz6lckYcgAa2rhXEPDRkecOlCOI, accessed 15 March 2024.

3 cdixon, 'Why Web 3 Matters', https://twitter.com/cdixon/status/1442201621266534402, (26 September 2021), accessed 15 March 2024, thread originated by @cdixon on Twitter (now X).

4 Jason Potts and Ellie Rennie, 'Web3 and the creative industries: how blockchains are reshaping business models', in Stuart Cunningham and Terry Flew (eds), *A Research Agenda for Creative Industries*, (Elgar 2019), 93-111.

5 European Commission Fintech Action Plan, 8 March 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109, accessed 15 March 2024.

Another recent trend is the widespread decoupling of use cases on distributed storage and transfer mechanisms such as distributed ledger technology (DLT). The decentralised storage and exchange of digital tokens, including through the use of DLT,[6] rely on a register or database split across an online network without a central control point.[7] Adding a further layer of complexity, many technologies are designed, developed and deployed on infrastructures or in spaces that remain beyond any single State's jurisdiction. The growing use of such distributed storage and transfer mechanisms has led to the validation and adoption of concrete, sector-specific use cases, as well as an acceleration of unique drivers of growth as a result of these use cases.[8] These can be seen in the expansion of DLT applications to various fields, including financial transactions, Internet of Things (IoT), and value and supply chains.[9] From cryptocurrency as the foundation of blockchain technologies relying on proof-of-work (PoW) protocol in Blockchain 1.0, Blockchain 2.0 moved on to smart contracts involving more financial functionality and decentralised applications with autonomously executing algorithms. This has further evolved into Blockchain 3.0, with larger-scale applications, improved performance, greater scalability and more interoperability, all rooted in proof-of-stake (PoS) protocol.[10]

---

6 See also the discussion about recent developments and trends in the digital economy, including DLT systems and applications, in HCCH, 'Developments with respect to PIL Implications of the Digital Economy', Prel. Doc. No 4 REV of January 2022, https://assets.hcch.net/docs/b06c28c5-d183-4d81-a663-f7bdb8f32dac.pdf, accessed 15 March 2024, paras 9-35.

7 UNCTAD, *Harnessing Blockchain for Sustainable Development: Prospects and Challenges*, (2021) UNCTAD/DLR/STICT/2021/3 and Corr. 1, p. 2.

8 See, *e.g.*, in the field of security in the Internet of Things, Anshul Jain, Tanya Singh and Nitesh Jain, 'Framework for Securing IoT Ecosystem Using Blockchain: Use Cases Suggesting Theoretical Architecture', in Milan Tuba, Shyam Akashe and Amit Joshi (eds), *ICT Systems and Sustainability,* (Springer 2020), 223-232.

9 Marketwatch, 'Blockchain market size analytical overview, demand, trends and forecast to 2024', (2019) https://www.marketwatch.com/press-release/blockchain-market-size-analytical-overview-demand-trends-and-forecast-to-2024-2019-04-05, accessed 15 March 2024.

10 "Proof of stake" refers to
"a consensus distribution algorithm which determines which users are eligible to add new blocks to the blockchain, thus, earning a cryptocurrency payment as mining fee. Using this method, of the users who participate in the mining process, those with more tokens are favoured over those with less".
UNCTAD, *Harnessing Blockchain for Sustainable Development: Prospects and Challenges*, *supra* note 7, 4 and 52.

Activities and interactions across jurisdictions and borders often expose gaps in the legal framework, giving rise to vulnerabilities due to questions of private international law (PIL) that arise. These include questions as to which authority has jurisdiction, which law is applicable, how decisions are recognised and enforced, and what cooperation mechanisms are available to overcome challenges of cross-border judicial or administrative procedures. The growing digitisation of the global economy and community exacerbates these vulnerabilities, as digital creations, actions, transactions and reactions online are, by a large majority, cross-border interactions. The vulnerabilities that arise in a digital habitat are a result of the borderless, mostly instantaneous, digital exchanges that take place between actors and participants in online platforms. The recent explosion of DLT-based and DLT-enabled transactions and interactions only serve to create greater digital vulnerabilities due to the anonymity or pseudonymity of actors and participants, the lack of an obvious connecting factor to *situs* for many transactions, and the lacunae that exist as a result of a lack of a uniform, harmonised PIL framework.

B. Digital vulnerability in the context of private international law

Vulnerability has emerged in various fields, from biomedical research and clinical medicine[11] to criminal justice,[12] as a core concept. The main idea is "an individual's (or a group's) propensity to suffer from physical or psychological harm".[13] From the perspective of legal scholarship, it can also be defined as the risk at which the rights of a person or group are violated.[14] Alarms have been sounded in the critical literature on vulnerability, with emphasis on the fact that the definition of vulnerability may either be too narrow (and hence run the risk of excluding individuals or groups

11 See generally Catriona Mackenzie, Wendy Rogers, Susan Dodds, *Vulnerability: New essays in ethics and feminist philosophy*, (2013: Oxford University Press); see also Samia A Hurst, 'Vulnerability in research and health care: describing the elephant in the room?', (2008) 22(4) Bioethics 191.

12 Robert Vargas, Kayla Preito-Hodge and Jeremy Christofferson, 'Digital Vulnerability: The Unequal Risk of E-Contact with the Criminal Justice System', (2019) 5(1) Russell Sage Foundation J Social Sciences 71.

13 Philipp Kellmeyer, 'Digital vulnerability: a new challenge in the age of super-convergent technologies', (2019) 12(1/2) Bioethica Forum 60 at p. 60.

14 Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition', (2018) 2(1) Yale J of Law and Feminism, 1-24.

that may be vulnerable), or too broad (thus leading to a situation where a particular individual may be categorised as vulnerable despite not being especially so).[15] Vulnerability is therefore often complex and layered,[16] and transposing specific kinds of vulnerability that apply to the individual onto groups or populations remains a challenge in many fields.

This is particularly evident in the case of digital vulnerability, especially where mapped on to institutional vulnerabilities. "Digital vulnerability" relates to the manner and means of human interaction with digital technologies.[17] The aligned and accelerated "super-convergence" of complementary key digital technologies creates digital vulnerability as a result of the pervasiveness and ubiquity of their use.[18]

Digital vulnerabilities arise as specific PIL challenges in the different sectors of the digital economy. These include:

- applicable law and choice of law (*e.g.*, what is the most appropriate connecting factor defining the law applicable to a transaction on a cross-border online platform, or via blockchain);
- jurisdiction and choice of court (*e.g.*, how to determine the competent court to resolve a dispute in relation to a non-fungible token (NFT) transacted within an immersive technology platform);
- recognition and enforcement (*e.g.*, how to enforce a foreign judicial decision in relation to a service regulated by a smart contract); and
- cross-border and cross-platform cooperation mechanisms (*e.g.*, what cooperation frameworks are feasible and desirable to overcome challenges that the digital economy faces).

15 Catriona Mackenzie, Wendy Rogers, Susan Dodds, *supra* note 11.

16 Florencia Luna, 'Elucidating the concept of vulnerability: Layers not labels', (2009) 2(1) Int'l J of Feminist Approaches to Bioeithcs 121.

17 Such as the consequences, both legal and institutional, of deceptive illusions through immersive technologies, Philipp Kellmeyer, Nicola Biller-Andorno, Gerben Meynen, 'Ethical tensions of virtual reality treatment in vulnerable patients', (August 2019) 25(8) Nature Medicine 1185; see *infra* section C., VI.

18 Philipp Kellmeyer, *supra* note 13, 60.

C. Practical use cases: answering private international law challenges to address digital vulnerability

Digital vulnerabilities that arise in the form of challenges to PIL are best illustrated in the practical use cases that abound in the digital economy today.[19] The protection of the rights of individuals, groups, businesses and communities begins with the question as to which framework of laws would be applicable, and run through to the question of which forum would be competent to hear a dispute, and how any resolution by the forum of such dispute would have practical effect. These form the classic trifecta of questions relating to applicable law, jurisdiction, and recognition and enforcement to which PIL addresses itself. In short, digital vulnerabilities arise because there is currently no harmonised framework that answers the what (law applies), when (such law should apply), who (should hear a dispute), and how (would parties have the opportunity to choose the law or forum) questions. From a PIL perspective, it is the *where* question (the *situs*) that may have traditionally aided in answering these other questions. It is the complexity – in some cases the impossibility – of answering the *where* question that gives rise to digital vulnerability.

The use cases that this section will examine are: (I) distributed storage mechanisms; (II) digital currencies and cross-border payments; (III) the tokenised economy; (IV) digital platforms; (V) artificial intelligence (AI) and automated contracting; (VI) immersive technologies and the cloud economy; and (VII) decentralised governance structures.

I. Distributed storage mechanisms

Increasingly, items and transactions take place online on distributed storage mechanisms, many of which are enabled by DLT. DLT has been defined as

19 See for more information in relation to studies undertaken on PIL aspects of these practical use cases, HCCH, 'Digital Economy and the HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference): Report', Prel. Doc. No 3A of January 2023, https://assets.hcch.net/docs/a61a1225-2eb0-4fef-8a7e-24ca186b5919.pdf, accessed 15 March 2024; HCCH, 'Private International Law Aspects of the Digital Economy: Report', Prel. Doc. No 5A of February 2024, https://assets.hcch.net/docs/b74f3bfe-51dd-4d0e-8d4b-59e5e32367da.pdf, accessed 15 March 2024.

> "...the practice that uses nodes...to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger). The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes".[20]

DLT is the protocol on which blockchain applications are based. A register of payments ("ledger") distributed across an online network without a central control point is created by blockchain technology.[21] A network of computers cryptographically identifies users and validates interactions among them before recording the interactions across the network of identifying and validating computers.[22] Entities interacting through the system are identified with a pair of cryptographic keys: a public key that acts like an address, and a private key that acts like a password. Each computer connected to the blockchain network is referred to as a node. Each of these nodes operates a full copy of validated transactions of the blockchain ledger.[23] Packages of data that carry the recorded data on the network are called "blocks". [24] Each block is definitively linked to the next block using a cryptographic signature, creating a "chain". This allows "blockchains" to act as a ledger that can be accessed and shared with the appropriate permissions.[25]

There are many ways of designing, implementing and employing DLT, which may be very different from the model used for blockchain. The unique design characteristics of DLT-enabled or DLT-native transactions

20 UNCTAD, *supra* note 7, 50.
21 *Ibid.,* 2.
22 See, *e.g.*, Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008), https://bitcoin.org/bitcoin.pdf, accessed 15 March 2024, (the Bitcoin Whitepaper, explaining the basics of blockchains); Vitalik Buterin, 'A next-generation smart contract and decentralized application platform', (2013), https://finpedia.vn/wp-content/uploads/2022/02/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, accessed 15 March 2024, (the Ethereum Whitepaper, elaborating on the functioning of blockchains as well as smart contracts).
23 UNCTAD, *supra* note 7, 51.
24 *Ibid*., 50.
25 *Ibid.*

and systems strain the application of traditional connecting factors.[26] Traditional connecting factors are difficult to apply to these technologies, with technological and legal challenges based on the pseudonymity of users, the immaterial nature of digital assets, the uncertainty of the location of network nodes and the online or decentralised nature of the platforms, making it difficult, or perhaps impossible, to determine the *situs* of a participant, item or transaction.[27]

Some DLT-enabled platforms further complicate the matter by resisting formal regulation in favour of self-regulation or adherence to the ethos of *lex cryptographica*.[28] Other PIL issues that arise in DLT use cases include:[29]

- the characterisation of, and law applicable to, the relationship between participants in a DLT system, including between asset holders and intermediaries such as crypto-exchanges and wallet providers;
- the law applicable to, the holding and transacting of assets in a DLT system;
- the jurisdiction of courts to hear disputes related to the outcomes of self-executing smart contracts deployed in DLT systems;
- the recognition and enforcement of DLT-based dispute resolution outcomes; and
- the question of how to determine the law applicable to tokens linked to real-world assets.

---

26 HCCH, Prel. Doc. No 3A of January 2023, *supra* note 19. See also the discussion about connecting factors in relation to digital assets created and transferred via decentralised systems, in HCCH, 'Developments with respect to PIL implications of the digital economy, including DLT', Prel. Doc. No 4 of November 2020, https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf, accessed 15 March 2024, paras 15-21.

27 Matthias Lehmann, 'Who Owns Bitcoin? Private (International) Law Facing the Blockchain', (2019) 42 *European Banking Institute Working Paper Series 2019*, 2.

28 See, *e.g.*, Primavera de Fillippi and Aaron Wright, *Blockchain and the Law – The Rule of Code* (Harvard University Press 2018). For an opposite view, see David Sindres, 'Is Bitcoin out of Reach for Private International Law?', in Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill Nijhoff 2023) 81.

29 Gérardine Goh Escolar, 'The Role and Prospects of Private International Law Harmonisation in the Area of DLT', in Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill Nijhoff 2023) 10. See also the discussion about the different PIL implications of permissioned and permissionless systems, in HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26, para. 16 and Annex I.

The characteristics of each DLT system impact the use cases best suited to it and raise different PIL issues.[30] Without an explicit choice of the applicable law, obstacles to the application of traditional objective connecting factors include the pseudonymity of the users and the inability to locate the DLT platform's connections to a certain jurisdiction, though some authorities have made attempts to do so based on the concentration of nodes.[31] While the explicit determination of the applicable law in an online platform agreement would be ideal, it does not consistently account for circumstances where users choose to avoid the services of a centralised platform, for reasons including security concerns, lack of platform trust, and personal philosophy. This has led to differing views as to whether analogies can be drawn from legal frameworks in existing regimes such as intellectual property[32] or goodwill in a business,[33] or whether an entirely new approach should be taken.[34] Moreover, the regulatory perimeters of many domestic legal institutions have been deemed to be insufficient to address the difficulties raised by the cross-border nature of DLT-enabled systems and applications. The larger-scale applications serviced by Blockchain 3.0 may also mean that "[n]o one solution can fit all DLT systems".[35]

30 On the use case analysis of DLT by asset class and product line, see World Economic Forum, *Digital Assets, Distributed Ledger Technology and the Future of Capital Markets: Insight Report*, (May 2021) https://www3.weforum.org/docs/WEF_Digital_Assets_Distributed_Ledger_Technology_2021.pdf, accessed 15 March 2024, 32-86.

31 Matthias Lehmann, 'Who Owns Bitcoin? Private (International) Law Facing the Blockchain', (2019), *supra* note 27.

32 Gerald Spindler, 'Fintech, digitalization, and the law applicable to proprietary effects of transactions in securities (tokens): a European perspective', (2019) 24 ULR 336, 337.

33 Andrew Dickinson (2019), 'Cryptocurrencies and the Conflict of Laws', in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019), paras 5.107–5.121.

34 See generally Michael Ng, 'Choice of law for property issues regarding Bitcoin under English law', (2019) 15(2) J Private Intl Law 316.

35 Financial Markets Law Committee (2018), *Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty*, (2018), 21.

II. Digital currencies and cross-border payments

Digital currencies are a "digital version of cash, controlled by a private cryptographic key – a unique random string of numbers".[36] Digital currency is owned by the holder of the private key associated with the relevant crypto wallet, which is used to hold and transfer the currency. There are currently three types of digital currencies: Cryptocurrencies (*e.g.* Bitcoin, Ethereum, Solana); StableCoins (*e.g.* Diem, formerly Libra), which are backed by a reserve asset such as fiat currency[37] held by banks; and Central Bank Digital Currencies (CBDCs), which are digital versions of fiat issued by a country's central bank.

In relation to cryptocurrencies, specific objections have been raised to the application of traditional PIL frameworks to legal relationships involving the use of cryptocurrencies. Arguments include views that these relationships are self-regulated and are subject to the *lex cryptographica* as opposed to legal regulation such as *lex mecatoria*,[38] or that there are major obstacles to the application of PIL in this field, including the delocalisation of transactions and the pseudonymity of actors.[39] Objections have been framed along two lines – either by viewing cryptocurrencies as assets in the sense of intangible movable property or by viewing cryptocurrencies as currency, and applying PIL by analogy.[40] Some commentators have moreover argued that the rapid evolution and diversification of the crypto asset and cryptocurrency landscape means that choice of law rules should offer "a sufficient degree of flexibility along with legal foreseeability and

36 Visa, 'The Crypto Phenomenon: Consumer Attitudes & Usage', (2021) https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-crypto-consumer-perceptions-white-paper.pdf, accessed 15 March 2024, 7.

37 "Fiat currency" refers to "any legal tender designated and issued by a central authority that people are willing to accept in exchange for goods and services because it is backed by regulation and because they trust this central authority". Consultative Group to Assist the Poor, World Bank, 'Bitcoin versus Electronic Money', (2014) https://documents1.worldbank.org/curated/en/455961468152724527/pdf/881640BRI0Box30WLEDGENOTES0Jan02014.pdf, accessed 15 March 2024, 1.

38 See *supra* note 28.

39 See, *e.g.*, M. Audit, 'Le droit international privé confronté à la blockchain', (2020) Rev crit DIP 669, 689.

40 See, *e.g.*, David Sindres, 'Is Bitcoin out of Reach for Private International Law?', *supra* note 28.

certainty".[41] Here, one solution may be to allow for the principle of party autonomy in choice of law,[42] which would enable parties to agree on the law governing the relationship between them, while accepting that there may be certain limitations on the freedom of choice in this context.[43]

On the other hand, CBDCs are digital currencies[44] issued by central banks, which include as key features: (1) the designation as a central bank liability; (2) denomination in an existing unit of account; and (3) use as a medium of exchange and a store of value.[45] Countries may have different objectives in issuing CBDCs, which include improving access to payments and promoting financial inclusion, increasing payment system competition, efficiency, and resilience, as well as safeguarding monetary sovereignty, and monetary and financial stability.[46] In 2022, it was estimated that 93% of central banks were exploring CBDCs, and that 58% were considering issuing a retail CBDC in either the short or medium term.[47] Use cases of CBDCs in finance, trade and digitised commerce include cross-border payments, e-commerce, machine-to-machine transactions and smart contracts.

41 Burcu Yüksel Ripley and Florian Heindler, 'The Law Applicable to Crypto Assets: What Policy Choices are Ahead of Us?', in Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill Nijhoff 2023) 259.

42 Simoen C Symeonides, *Codifying Choice of Law Around the World: An International Comparative Analysis*, (Oxford University Press 2014), Chapter 3.

43 See, *e.g.*, HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26, Annex I.

44 The Bank for International Settlements (BIS) provides a succinct explanation of CBDCs, noting that there are two types of CBDCs, "[r]etail CBDCs (rCBDCs) are intended for the general public, aiming to provide a risk-free and digital means of payment for everyday transactions. Wholesale CBDCs (wCBDCs), on the other hand, are designed for use among financial intermediaries and operate like central bank reserves but with added functionalities enabled by tokenisation". See BIS / FSI Connect, "Central bank digital currencies – Executive Summary", undated, https://www.bis.org/fsi/fsisummaries/cbdcs.pdf, accessed 15 March 2024.

45 IMF WP/20/254, 'Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations', (November 2020), 6. A possible indirect structure is the issuance of the liability by a commercial bank which in turn is fully backed with central bank liabilities. This structure is not deemed as a genuine CBDC by some experts, because in the case of bankruptcy of the commercial bank the user would have a claim against such commercial bank, not against the central bank.

46 Gabriel Soderberg, *et al.*, IMF NOTE/2023/008, 'How should central banks explore central bank digital currency?' (September 2023), https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504, accessed 15 March 2024, 9-11.

47 BIS, BIS PAPER/23/136, 'Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto', (2023), 4 and 9.

A PIL analysis of the use of CBDCs could generally start with the use of traditional connecting factors. Potential connecting factors may depend on the infrastructure where a CBDC is issued. For example, a possible infrastructure could be on a distributed ledger located in multiple jurisdictions and without either a central authority or validation point, where applying the *lex situs* or the Place of Relevant Intermediary Approach (PRIMA) principle as a connecting factor may be difficult, especially in relation to intangible assets held therein.[48] While the implications of a certain infrastructure can presumably be clarified by the supervision of the central bank or another authority that is able to designate an applicable law to the system, the *situs* becomes less clear where, for example, the central bank's role is limited to identity verification or where technical ledger access and intermediaries play a greater role.[49] Other connecting factors include the law chosen by the DLT network participants (*elective situs*), the law approved by regulators (*modified elective situs*), the residence of the participant who is transferring the CBDC or the residence of the encryption private master key-holder for the DLT system (PREMA).[50]

The legal nature of CBDCs might also pose challenges to applying conventional PIL rules.[51] Even if rules are found to apply, it is not clear whether every existing rule is fit for purpose. For example, if a CBDC is classified as a tangible-intangible hybrid under a domestic legal framework, the *lex rei sitae* could in theory apply, but it is unclear what the *situs* of a token held on distributed registers and through wallets would be.[52]

CBDCs have the potential to alleviate existing frictions caused by a lack of interoperability, standardisation, as well as other challenges (*e.g.*, high number of intermediaries) in cross-border payments,[53] which are financial transactions where the payer and the recipient are based in different

48 See HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26.

49 See HCCH, 'Exploratory Work: Private International Law Aspects of Central Bank Digital Currencies (CBDCs)', Prel. Doc. No 4 of January 2024, https://assets.hcch.net/docs/410f9f34-3360-4d22-87ff-0876377a3d87.pdf, accessed 15 March 2024, Annex III. An example is Project Tourbillon, see Annex IV.

50 *Ibid.* Previous exploratory work carried out by the Permanent Bureau of the HCCH already has identified connecting factors in the context of digital economy, including DLT, and could be a relevant input for future work, see Annex I, HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26.

51 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49, para. 55.

52 *Ibid.*

53 BIS, BIS Report to the G20 *Central bank digital currencies for cross-border payments*, (July 2021), 13-14.

jurisdictions.[54] Here again, PIL challenges will need to be answered. An example is the issuance and use of a CBDC as a digital token without a current-account relationship between the central bank and the holder,[55] and where intermediaries may provide services such as holding wallets and handling payments for users.[56] Many national legislations do not recognise CBDCs as a form of digital asset, as CBDCs and digital assets serve different purposes and have different legal implications.[57] As such, crucial legal implications arise in the design choices underlying a CBDC.[58]

Depending on the chosen design and model of operation, particularly in relation to cross-border CBDC access by non-residents, central banks may delegate functions to private sector intermediaries.[59] Deployment of national CBDCs may also potentially require the use of foreign intermediaries, or intermediaries with worldwide offices; moreover, a user may hold CBDCs of different jurisdictions in the same account. Intermediaries provide necessary services for the operation and implementation of CBDCs but the functions delegated to them, their location, and their method of integration into the CBDC system may raise PIL issues. Intermediaries may be afforded varying degrees of functionality and independence depending on how they are included in the technical framework of a CBDC cross-border payment system, leading to complexities in the analysis of *situs*. Thus, the PIL implications resemble the intermediation and dematerialisation challenges that informed the development of the *Convention of 5 July 2006 on the Law Ap-*

54 IMF NOTE/2023/008, *supra* note 46, 10, 20-21, about CBDCs used for cross-border payments.

55 IMF, IMF WP/20/254 *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*, (November 2020), 9.

56 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49. It may be too challenging for central banks to assume such tasks. Accordingly, intermediaries, such as commercial banks and financial institutions, are considered as more suitable for it.

57 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49.

58 In WP/20/254, *supra* note 55, 10-11. the IMF has identified these choices on CBDC design in terms of dichotomies between account-based vs. token-based; wholesale vs. retail; direct vs. indirect; and centralised vs. decentralised. In addition, in IMF NOTE/2023/008, *supra* note 46, 18-19, the IMF noted that different principles may be considered to assess the design options, such as interoperability, compliance with the laws and regulations, resiliency, upgradability, and others.

59 BIS, *Options for access and interoperability of CBDC for cross-border payments*, (2022), https://www.bis.org/publ/othp52.pdf, accessed 15 March 2024.

plicable to Certain Rights in Respect of Securities held with an Intermediary (HCCH Securities Convention).[60]

Clarity as to applicable law considerations in payment systems interoperability would enable payments service providers to make payments across systems without concerns as to payments law and settlement finality. As CBDCs systems used for payments would have similarities with existing payments infrastructure, existing payments law may be a useful starting point for establishing PIL considerations.[61]

However, the specific features of CBDCs do not allow the PIL frameworks that already exist for cash payments to apply one-to-one. For example, the *lex monetae* could prevail over party autonomy when determining the applicable law for some issues. Additionally, the participation of intermediaries would have an impact on the PIL analysis. Recipient countries of a foreign CBDC could decide the extent to which they will authorise the denomination of contracts in foreign currency, and recipient countries' treatment of a foreign CBDC is likely to be affected by the issuing country's rules regarding that CBDC.[62] These PIL challenges would arise in both wholesale retail payments within the specific context of each country or jurisdiction.[63] Notably, the roles and responsibilities of intermediaries in cross-border payments and the status of intermediaries in cross-border insolvency regimes are issues that should be considered in any PIL analysis.[64]

60 HCCH *Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary*, https://assets.hcch.net/docs/3afb8418-7eb7-4a0c-af85-c4f35995bb8a.pdf, accessed 15 March 2024.

61 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49.

62 Heng Wang, 'How to Understand China's Approach to Central Bank Digital Currency', (2023) 50 Computer Law and Security Rev 1, 24. Such PIL considerations, of course, would be subject to overriding mandatory regulations and other overriding considerations including monetary sovereignty, foreign exchange policies, and other regulatory and compliance requirements.

63 There are pilots on both use cases: wholesale payments and retail payments. Cross border pilots have been mostly focused on wholesale payments, in collaborative projects carried out by groups of central banks. Moreover, some central banks are more active in implementation or experimentation of CBDC pilots, while others are more cautious. These differences are mainly explained because the design of a CBDC needs to address the specific context of each country, and some central banks have not identified the need to introduce a CBDC, thus conducting monitoring activities while others prefer the involvement of private parties (*e.g.,* commercial banks) in more advanced stages. Regarding the country-specific circumstances to be considered for a CBDC design, see BIS Innovation Hub, 'Project Polaris Part 4: A high-level design guide for offline payments with CBDC', (October 2023), 33-37.

64 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49.

III. The tokenised economy

Digital tokenisation allows tangible and intangible objects, rights and claims to be virtually represented and stored electronically, usually in distributed storage mechanisms. While recognising the lack of such a definition, the BIS notes that tokenisation refers to the digital representation of value or rights.[65] Tokenisation can be an enabler of fast and secure transactions, including transfers, tracking and management of tokenised value or rights across borders. According to the BIS, tokenisation streamlines transactions, reducing the need for intermediaries and increasing the transparency and security of these transactions. Consequently, digital tokenisation has become one of the most prominent use cases of distributed storage mechanisms in financial and capital markets in many jurisdictions.

Three trends are of particular interest.

The first trend is the digital tokenisation of real-world assets by the creation of a virtual representation of existing tangible assets,[66] storing these virtual representations on decentralised or distributed storage mechanisms (for example, using DLT), and conventionally embedding their value and any rights or obligations associated with the real-world asset in the virtual representation.[67] This may include the representation on DLT of traditional asset classes such as financial instruments, collateral or real assets.[68] The relevant real-world assets, in particular where they are tangible assets, would typically be placed in custody to ensure continuous backing for the

65 BIS, Annual Economic Report Part III, (June 2023) https://www.bis.org/publ/arpdf/ar2023e3.pdf, accessed 15 March 2024, 89.

66 Garrick Hilleman and Michel Rauchs, Global Blockchain Benchmarking Study, (2017) https://dx.doi.org/10.2139/ssrn.3040224, accessed 15 March 2024, 51 and 64.

67 *Ibid*., see also Iñaki Aldasoro *et al*., The tokenisation continuum, 11 April 2023, https://www.bis.org/publ/bisbull72.pdf, accessed 15 March 2024, 1, 3. Tokenisation may include, for example, "the representation of pre-existing real assets on the ledger by linking or embedding by convention the economic value and rights derived from these assets into digital tokens", see Organisation for Economic Co-operation and Development (OECD), *The Tokenization of Assets and Potential Implications for Financial Markets*, (2020) OECD Blockchain Policy Series, https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm, accessed 15 March 2024, 11.

68 See, for example, Financial Stability Board (FSB), *Decentralised financial technologies: Report on financial stability, regulatory and governance implications*, (2019), https://www.fsb.org/wp-content/uploads/P060619.pdf, accessed 15 March 2024.

digital tokens. Tokenisation is currently being piloted for various real-world assets, such as real estate.[69]

According to the OECD,

> "[t]he application of DLTs and smart contracts in asset tokenisation has the potential to deliver a number of benefits, including efficiency gains driven by automation and disintermediation; transparency; improved liquidity potential and tradability of assets with near-absent liquidity by adding liquidity to currently illiquid assets; faster and potentially more efficient clearing and settlement. It allows for fractional ownership of assets which, in turn, could lower barriers to investment and promote more inclusive access by retail investors to previously unaffordable or insufficiently divisive asset classes, allowing global pools of capital to reach parts of the financial markets previously reserved to large investors".[70]

Nevertheless, the OECD goes on to note that the large-scale adoption of asset tokenisation would face "governance risks related to AML/CFT;[71] digital identity issues; and data protection and privacy issues; as well as rais[e] questions about the legal status of smart contracts".[72] Questions relating to the characterisation of such tokens for PIL purposes, and the significant role of custodianship of assets that have been tokenised, will necessarily arise.

An example of such asset tokenisation relates to NFTs. NFTs form a class of digital asset or token that can be proved to be unique, meaning that it is not interchangeable (*i.e.* "non-fungible") with another digital asset token. The uniqueness, transparency and provability of ownership, and asset programmability of the NFT is usually cryptographically, immutably and publicly recorded on a distributed ledger.[73] The European Union Blockchain Observatory and Forum has noted that indicative NFT use

69 OECD, *The Tokenization of Assets and Potential Implications for Financial Markets*, (2020), *supra* note 67.

70 *Ibid*., 7.

71 AML/CFT is the acronym for "anti-money laundering/combating the financing of terrorism".

72 OECD, *The Tokenization of Assets and Potential Implications for Financial Markets*, (2020), *supra* note 67, 7.

73 EU Blockchain Observatory and Forum, 'Demystifying Non-Fungible Tokens (NFTs)' (November 2021), 4-5.

cases include digital art[74] (including gaming collectibles),[75] supply chain logistics,[76] content ownership,[77] and assets in immersive technologies.[78]

A specific issue that NFTs face is the recognition and enforcement of the underlying mechanism used for transferring and establishing ownership. While some have opined that NFTs are property deeds that give an ownership title to a physical asset,[79] the deed or title entitles the holder to ownership of the asset and is not the asset itself. The purchase of an NFT gives ownership of the NFT itself, with any further rights or entitlements decided by the terms of the token smart contract. This raises the question of the characterisation of NFT transactions – whether they are solely contractual, or whether they carry proprietary characteristics. Other issues

74 See, *e.g.*, Beeple (2021), 'Everydays: The First 5000 Days', minted on 16 February 2021 and sold at online auction on 11 March 2021 for in excess of USD 69 million, https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924, accessed 15 March 2024.

75 See, *e.g.*, Cryptokitties, backed on the Ethereum blockchain, which allows players to breed digital kitties in-game to be traded via the use of NFTs, https://www.cryptokitties.co/, accessed 15 March 2024.

76 See, *e.g.*, Nike's Cryptokicks project, for which it secured a patent, that stores unique identifiers given to each pair of shoes, https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=Nike&s2=Crypto&OS=Nike+AND+Crypto&RS=Nike+AND+Crypto, accessed 15 March 2024.

77 See, *e.g.*, Audius, a decentralised audio streaming and sharing platform on the blockchain, https://audius.co/, accessed 15 March 2024.

78 See, *e.g.*, sales of digital land in the Sandbox and Decentraland, Cointelegraph, 'Virtual land in the metaverse dominated NFT sales over past week' (6 December 2021), https://cointelegraph.com/news/virtual-land-in-the-metaverse-dominated-nft-sales-over-past-week, accessed 15 March 2024.

79 Jeremy Goldman, 'A Primer on NFTs and Intellectual Property' (March 2021), https://www.lexology.com/library/detail.aspx?g=d96ed012-8789-4e87-bc1d-70ba76569c0f, accessed 15 March 2024.

that arise in regard of characterisation is whether NFTs can be considered commodities,[80] securities,[81] or intellectual property.[82]

The second trend relates to the focus on fund tokenisation. These "digital funds" issue tokenised shares or units that represent investor interests, which are recorded and traded on distributed platforms rather than in the traditional registries or record-keeping systems.[83] Such digital funds have gained traction in leading fund jurisdictions worldwide, including France, Germany, Luxembourg, Singapore and the United States of America.[84] An example of a cross-jurisdictional tokenised fund is the collaboration between the BIS Innovation Hub, the Swiss National Bank, the World Bank and the International Monetary Fund (IMF) to tokenise development funds, with the goal of promoting global economic development.[85]

The digital nature of these tokenised funds, compounded by their storage on distributed storage mechanisms, raises issues of localisation that have an impact on the PIL analysis. The variety of actors and participants in transactions involving digital tokens may challenge the application of traditional connecting factors, as there may be several objective connecting factors to a number of jurisdictions. The digital nature of this field also means that transactions may occur, and participants may be sited, in different jurisdic-

80 See, *e.g.*, the U.S. Commodity Futures Trading Commission (CFTC), CFTC (2020), *Digital Assets Primer,* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi0uoe5_Ob0AhWp7rsIHc9ODKAQFnoECCAQAQ&url=https%3A%2F%2Fwww.cftc.gov%2Fmedia%2F5476%2FDigitalAssetsPrimer%2Fdownload&usg=AOvVaw0ldGq63IE48QOEzXajIyBa, accessed 15 March 2024.

81 See, *e.g.*, the position of the U.S. Securities and Exchange Commission (SEC), SEC (2021), 'Framework for 'Investment Contract' Analysis of Digital Assets', https://www.sec.gov/files/dlt-framework.pdf, accessed 15 March 2024.

82 Amy Madison Luo, 'NFTs: A Legal Guide for Creators and Collectors', (11 March 2021), https://www.coindesk.com/policy/2021/03/11/nfts-a-legal-guide-for-creators-and-collectors/, accessed 15 March 2024.

83 Investment Association, *UK Fund Tokenisation: A Blueprint for Implementation. Interim Report from the Technology Working Group to the Asset Management Taskforce*, (November 2023), https://www.theia.org/sites/default/files/2023-11/UK%20Fund%20Tokenisation%20-%20A%20Blueprint%20for%20Implementation.pdf, accessed 15 March 2024, 9.

84 *Ibid*., p. 16.

85 Cecilia Skingsley, Head of the BIS Innovation Hub, 'Shaping the future financial system in the public interest', Keynote Speech at the Conference "Exploring central bank digital currency: Evaluating challenges & developing international standards", (28 November 2023), Washington DC, https://www.bis.org/speeches/sp231128.htm, accessed 15 March 2024, para. 50.

tions and locations. PIL questions regarding which law would be applicable and which forum would have jurisdiction would necessarily arise.

The third trend relates to the tokenisation of identity-bound data. This finds its use case in the issuance of soulbound tokens.[86] Soulbound tokens are defined as publicly-visible, non-transferable tokens representing affiliations, memberships, and credentials, enabling a digital DLT wallet to act as an "extended resumé" of the holder's activities and relationships.[87] Illustrations include tokens issued by a university to certify that the wallet holder is a graduate, tokens providing proof of substantial relationships such as participation in the governance of decentralised autonomous organisations (DAOs), and tokens used to model traditional financial systems and arrangements.

These soulbound tokens provide a digital method of representing a wallet holder's location, personal identification, or affiliations. An elaborated arrangement of soulbound tokens could provide an indication of real-world identities, locations, places of business, and patterns of social or economic behaviour, all of which are facts that facilitate the application of traditional connecting factors. Furthermore, users would be incentivised to voluntarily acquire more soulbound tokens because their possession can signal the authenticity of their own digital wallets and the consistency and reliability of their performance of obligations. Such markers of reliability in a wallet would facilitate access to more privileges for the holder. For this reason, soulbound tokens may overcome the location- and identity-based barriers of PIL and DLT, while respecting the ethos of peer-to-peer exchange that guides many DLT communities.

86 E. Glen Weyl, Puja Ohlhaver, Vitalik Buterin, 'Decentralized Society: Finding Web3's Soul', (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763, accessed 15 March 2024.

87 The term "Soulbound" is borrowed from massively multiplayer online games, where Soulbound equipment is typically rewarded for accomplishments of high complexity and time investment, and is "bound" to the player's "soul" because it cannot be traded or sold to other players. The equipment therefore has reputational value because it proves that the owner accomplished a significant challenge in the game.

IV. Digital platforms

Digital platforms refer to "digital infrastructure enabling interaction among multiple groups".[88] Digital platforms operate across varied sectors, enabling different types of interactions between different categories of parties. PIL issues manifest in various ways in the platform economy, depending on the relationships that arise:[89]

- Between the platform and the user: The relationship between the platform and the user typically is contractual and, of relevance to PIL, typically relies on choice of law clauses;
- Between users: Questions arise where there is no valid choice of law, as is often the case in peer-to-peer digital environments;
- Between the platform and / or its user, and the non-user: Where there are no pre-existing relationships between these parties, questions may arise where a harm is done to the non-user, in particular in relation to tortious claims. There may also be questions in relation to the law applicable to the determination of the liability of intermediaries.[90]

In relationships between platforms and their users, three specific PIL issues arise. First, the determination of the law applicable to contracts between the platform and the user is generally straightforward. However, tortious matters give rise to questions of the law applicable, as a rule for the law applicable based on the place of the user's location or the user's habitual residence may conflict with the contractual terms of the platform. Second, there is an increasing number of cases that are being litigated between aggrieved users and online platforms in which user-plaintiffs have argued that, where they have suffered a wrong done by another user, platform hosts are obliged to either sanction the (allegedly) offending user or otherwise remedy the wrong. The question that arises is whether choice of court and choice of law clauses in contracts entered into between users and the relevant digital platforms may go some way towards resolving such questions.[91] Third, and perhaps most significant in the discussion of digital

88 See Dai Yokomizo, 'Digital Platforms and Conflict of Laws', (2021) 64 Japanese Yb of Int'l Law 202, 202.

89 See Tobias Lutzi, 'Private ordering, the platform economy and the regulatory potential of private international law', in Ilaria Pretelli (ed.) *Conflict of Laws in the maze of digital platforms*, (Schultess: 2018), 129-143.

90 See Dai Yokomizo, *supra* note 88, 216.

91 *See* Tobias Lutzi, *supra* note 89, 134.

vulnerability, while some jurisdictions have specific PIL rules that protect weaker parties such as consumers and employees, these sector-specific rules do not apply to protect the small and medium-sized enterprises that also take part in transactions on digital platforms, leaving a lacuna in the PIL framework.[92]

The fastest-growing use case of digital platforms, in particular on distributed storage mechanisms, is decentralised finance (DeFi). DeFi platforms bring together a wide spectrum of financial market participants and has been attracting significant capital and liquidity pools in the international and cross-border financial ecosystem. DLT-enabled DeFi platforms operate without a centralised authority or physical presence, and their transactions can be executed automatically, thereby imposing challenges in connecting a transaction on a DeFi platform to a location for the determination of jurisdiction and applicable law through the use of traditional connecting factors.

V. Artificial intelligence and automated contracting

The adoption of AI in applications, in particular generative AI, has led to innovations in various fields, such as automated contracting. While automated contracting is not new, having been the basis of applications such as point-of-sale systems and electronic data interchange (EDI) for many decades, the use of automated contracting in smart contracts, computable contracts, and algorithmic contracts has meant an increased reliance on AI in both commercial and end-user contracts. In particular, transactions conducted on online platforms and smart devices (including high-frequency trading transactions) can involve interactions between a human and an automated system, or interactions between automated systems. Automation at the different stages of the contract life cycle, together with the automation of stages in the contract life cycle from drafting to negotiation and

92 Most of these laws enable the use of a specific mandatory rule of law from the jurisdiction in which these weaker parties are habitually resident, see Dai Yokonizo, *supra* note 88, 225.

management to analysis,[93] allow for the streamlining and systematising of cross-border contracting on digital platforms.

Developments in AI and automated contracting have raised several PIL questions. First, when AI-enabled technologies perform acts or take part in transactions, the online nature of most AI-enabled systems may make traditional connecting factors inapplicable. Second, the use of AI-enabled systems may make determining jurisdiction difficult due to the challenges in determining location in online platforms (including the application of the *forum non conveniens* doctrine, where relevant). Another challenge relates to the identification of the type of harm that an AI-enabled system may cause, and to the localisation of such harm, since traditionally *situs*-based PIL connecting factors may not be useful in linking the occurrence of the damage to a certain jurisdiction. For example, a generative AI-enabled networked system not localised to a particular *situs* may scrape data from one website in a particular jurisdiction in order to generate content on another website sited elsewhere.[94] Third, the enforcement of foreign judgments may be challenging as a result of different approaches to AI-enabled systems. Some jurisdictions may see public policy and other concerns presenting obstacles to the recognition and enforcement of decisions in situations where AI-enabled algorithms are involved, and where they are empowered to render final decisions.

VI. Immersive technologies and the cloud economy

Immersive technologies have created virtual multi-purpose platforms that are empowered by virtual and augmented reality and methods of transacting based on distributed storage mechanisms. Such platforms based on immersive technologies, in particular those native to the cloud, allow individuals, businesses and other entities to create, act, react and transact in relation to both real-world as well as virtual items. Immersive technologies have found applications in a range of use cases that include enter-

93 See Martin Ebers, 'Artificial Intelligence, contracting and contract law' in Martin Ebers, Cristina Poncibò, Mimi Zou (eds.), *Contracting and contract law in the age of artificial intelligence*, (2022: Bloomsbury) 102.

94 Marion Ho-Dac, and Cécile Pellegrini, *Governance of Artificial Intelligence in the European Union: What Place for Consumer Protection?*, (Bruylant: 2023), 303.

tainment,[95] gaming,[96] litigation and arbitration proceedings,[97] and digital communications.[98] Web3 immersive technology platforms are "emerging market virtual world economies with a continually developing complex mix of digital goods, services, and assets that generate real-world value for users".[99] These platforms create a new paradigm by eliminating capital controls and creating a "new free-market internet-native economy that can be monetised in the physical world",[100] a revenue opportunity that spans social commerce, digital events, hardware, and content monetisation.[101]

Immersive technologies raise PIL questions not only because of the nature of the networked platforms on which these technologies operate, but also as a result of the seamless connection between digital and real-world objects. Here, traditional connecting factors may not apply, leading to challenges in identifying the applicable law (which may address the platform as a whole, or may address a single transaction or user), and the possible anonymity or pseudonymity with which users interact in immersive technology platforms. It therefore becomes a challenge to connect events, assets,

95 For example, over 12 million users joined the Fortnite platform to watch a virtual concert by entertainer Travis Scott in April 2020, see Ji Hye Park, 'The Direction and Implications of the Content Industry in the Metaverse Era', (2022) 26(6) *KIET Industrial Economic Review* 55, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4194255, accessed 15 March 2024.

96 The number of monthly users of Roblox, an immersive technology game, exceeds 150 million, see Busra Alma Çalli and Cagla Ediz, 'Top concerns of user experiences in Metaverse games: a text-mining based approach', (May 2023), 46 Entertainment Computing, https://www.sciencedirect.com/science/article/abs/pii/S1875952123000319, accessed 15 March 2024.

97 Timothy T Hsieh *et al*., 'Intellectual Property in the Era of AI, Blockchain and Web 3.0', (March 2023), *Blockchain and Web* 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4392895, accessed 15 March 2024.

98 See generally Dale Mitchell, Ashley Pearson and Timothy D Peters (eds.), *Law, Video Games, Virtual Realities: Playing Law*, (Routledge 2024).

99 Grayscale Research, 'The Metaverse: Web 3.0 Virtual Cloud Economies' (2021), https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf, accessed 15 March 2024, 10.

100 *Ibid*., 7.

101 Grayscale Research, 'The Metaverse', *supra* note 99, 9 and 16. See also Pedro Palandrani, The Metaverse Takes Shape as Several Themes Converge, *Global X ETFs Research,* (13 September 2021), https://www.globalxetfs.com/content/files/The-Metaverse-Takes-Shape-as-Several-Themes-Converge.pdf, accessed 15 March 2024.

and actors where they may not have (validly) agreed on applicable laws and jurisdiction.[102]

Immersive technology at play in cloud economies raise questions in relation to the characterisation of the agents relating to sovereign virtual goods being transacted in the cloud. Questions arise as to the legal frameworks that are relevant, and the PIL implications of those legal frameworks. Perhaps most significant in relation to the use of immersive technologies in cloud economies is the increasing use of decentralised governance, including decentralised autonomous organisation (DAO) frameworks and their attendant voting mechanisms, community audits, and multisignature wallets.[103] Decentralised cloud services also mean that storage, computing, and databases are decentralised in the borderless cloud. The borderless nature of cloud economies finds itself in tension with the traditional significance of geographic *situs* in PIL.[104]

Another issue that arises in cloud economies and metaverses is the PIL implications of cross-border data transactions. While the general focus of regulators has thus far been on consumer privacy and the protection of personally identifiable data,[105] PIL questions relating to jurisdiction, applicable law and recognition will increasingly arise as more data transactions take place in the cloud and as certifications of data transactions are increasingly tokenised.

102 See generally European Parliament, Briefing: Metaverse Opportunities, risks and policy implications, (June 2022), https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf, accessed 15 March 2024; see also Grayscale Research, 'The Metaverse', *supra* note 99.

103 A "multisignature wallet" (also referred to as a "multigeniture wallet") refers to a cryptocurrency wallet that requires authentication from multiple parties to complete a transaction, which is the type of cryptocurrency wallet commonly used in DAOs, see, *e.g.*, Monika di Angelo and Gernot Salzer, 'Characteristics of Wallet Contracts on Ethereum', (2020) *IEEE* 1, 1-2. See *infra* section C., VII.

104 Dan Jerker B. Svantesson, 'The (uneasy) relationship between the HCCH and information technology', in Thomas John, Rishi Gulati, and Ben Kohler (eds), *The Elgar Companion to the Hague Conference on Private International Law* (Edward Elgar Publishing 2020), 462; see also Gérardine Goh Escolar, *supra* note 29.

105 Jin Huang, 'Applicable Law to Transnational Personal Data: Trends and Dynamics', (2020) German Law Journal 1285.

VII. Decentralised governance structures

Decentralised governance within distributed platforms may be managed by a community of members who have the right to propose initiatives through DAOs.[106] In order to pursue a purpose with minimal human intervention,[107] DAOs use coded smart contracts to set out the rules for what the purpose of the DAO is, how members agree to cooperate, how decisions are collectively taken through a voting process, how native tokens are created and distributed, and how transactions are executed once certain triggering conditions are met.[108]

A DAO is therefore a tool to achieve decentralised governance within DLT platforms, building community management features that include the pooling of tokens, voting, audits and multisignature wallets.[109] A DAO may have the potential to be characterised as a trust form, or at least to use the trust form as the closest analogy that may limit the liability of DAO members in the absence of a corporate form.[110] Trusts as a potential legal holding structure for assets of DAOs, as well as the legal recognition of DAOs as institutions analogous to trusts, may subject the recognition of DAOs to the mechanisms of the *Convention of 1 July 1985 on the Law Applicable to Trusts and on their Recognition* (HCCH Trusts Convention).[111] This may provide a potential method of providing legal recognition of DAOs across borders,

106 Sam Gabor and Noah Walters, 'Getting DAO to Business: Decentralized Autonomous Organizations Under Canadian Insolvency Law', (2022) 20th Annual Review of Insolvency Law, 2022 CanLIIDocs 4301.

107 Robert A Schwinger, 'Blockchain law: DAOs enter the spotlight', (2022) New York LJ 1, https://www.nortonrosefulbright.com/en-us/knowledge/publications/030cbf64/blockchain-law-daos-enter-the-spotlight, accessed 15 March 2024.

108 Robert Dobbyn, Rupert Morris and Marcel Treurnicht, 'Bridging the Gap – How Trusts Can Give DAOs a Foothold in the Traditional Economy', (18 March 2022), https://www.walkersglobal.com/index.php/publications/100-article/2947-bridging-the-gap-how-trusts-can-give-daos-a-foothold-in-the-traditional-economy?utm_source=mondaq&utm_medium=syndication&utm_term=Technology&utm_content=articleoriginal&utm_campaign=article, accessed 15 March 2024.

109 See *supra* note 103.

110 Carla Reyes, 'If Rockefeller Were a Coder', (2019) 87 George Washington LR 379.

111 HCCH *Convention of 1 July 1985 on the Law Applicable to Trusts and on their Recognition,* https://assets.hcch.net/docs/8618ed48-e52f-4d5c-93c1-56d58a610cf5.pdf, accessed 15 March 2024. See Alfred E. von Overbeck, "Explanatory Report on the 1985 Hague Trusts Convention", in *Proceedings of the Fifteenth Session* (1984), Tome II, *Trusts - applicable law and recognition*, (Imprimerie Nationale 1985), 370-415, paras 28-29.

relying on common characteristics such as being composed of community members with a common purpose; [112] a separate fund created in a digital environment;[113] and management through distributed governance among the members of the community.[114]

D. Conclusion

The concept of digital vulnerability cuts across sectors and communities, focusing on the individual or entity that finds itself at risk by virtue of the inherent characteristics of the digital platform on which they interact. In many ways, approaching the protection of these individuals and entities, as well as their rights, from a PIL perspective takes the same tack. By cutting across the plethora of applications, platforms and purposes in the digital economy, asking and addressing the PIL questions that arise in the digital habitat directly addresses and aims to resolve the challenges that arise with digital vulnerability. By addressing the questions of what (law applies), when (such law should apply), who (should hear a dispute), and how (would parties have the opportunity to choose the law or forum), steps taken to harmonise the global PIL framework in the digital economy tackle digital vulnerabilities head on, in concrete use case scenarios, and in relation to real-world situations. Answering these questions of private international law makes us all less vulnerable as natives in the digital world that we inhabit today.

112 Aaron Wright, 'The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges', (2021) 4(2) Stanford Journal of Blockchain Law & Policy 152, https://stanford-jblp.pubpub.org/pub/rise-of-daos/release/1, accessed 15 March 2024, 158.

113 *Ibid*., p. 156.

114 Carlos Santana and Laura Albareda, 'Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda', (October 2023) *Technological Forecasting and Social Change*, Vol. 182, September 2022; E. Naudts, 'The future of DAOs in finance - in need of legal status', European Central Bank Occasional Paper No 2023/331, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf, accessed 15 March 2024, 8-9.

Addressing Vulnerabilities in Online Dispute Resolution

Federica Casarosa, Hans-W. Micklitz

A. Introduction

'Vulnerability,' or maybe better 'vulnerabilities,' has become a catchword in the current debate on an appropriate legal design to handle the pros and cons of the digital economy.[1] It is also mentioned in the many regulations and draft regulations the EU has already adopted or is about to adopt in the current term of the European Parliament and the European Commission.[2] When linking 'vulnerabilities' to 'online dispute resolution (ODR),' three different strands of discourse come together:

– *Facilitating access to justice with out-of-court mechanisms which are more easily accessible by inexperienced citizens.*

1 Krupiy, T. (2020) 'A Vulnerability Analysis: Theorising the Impact of Artificial Intelligence Decision-Making Processes on Individuals, Society and Human Diversity from a Social Justice Perspective' 38 Computer Law & Security Review 105429; Malgieri, G. (2023) 'Assessing (and Mitigating) Layers of Data Subjects' Vulnerability: Using the DPIA as a Model' in Malgieri, G. *Vulnerability and Data Protection Law*; Calo, R. (2018) 'Privacy, Vulnerability, and Affordance' in Selinger, E., Polonetsky, J., and Tene. O. (eds), *The Cambridge Handbook of Consumer Privacy*; Albertson Fineman, M. (ed.), (2010) 'The Vulnerable Subject: Anchoring Equality in the Human Condition', *Transcending the Boundaries of Law*; Ippolito, F. (2021) 'Vulnerability and Fundamental Rights in the Area of Freedom, Security and Justice' in Iglesias Sánchez, S., and González Pascual. M. (eds), *Fundamental Rights in the EU Area of Freedom, Security and Justice*.

2 See the recent Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, OJ L 135, 23.5.2023, 1; Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC, OJ L, 2023/2225, 30.10.2023; Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023.

– *Protecting the weaker party in a contractual relationship with appropriate legal tools at the substantive level.*
– *Developing an appropriate design for vulnerable persons enables 'normal citizens,' and particularly vulnerable persons, to benefit from digitalisation and enjoy protection against possible risks.*

Only a holistic perspective taking the three strands into account – access to justice and out-of-court mechanisms, protection of the weaker party in the industrial economy and due consideration of potential vulnerabilities in the digital economy – allows identification of the central elements which must be considered when developing new online dispute resolution mechanisms. This contribution addresses the development of ODR mechanisms as tools to enhance access to justice and shows how this principle has shaped policy choices at the European level in legislative interventions. This requires including these legislative acts in the industrial and digital economy. In this field, the contribution focuses on the Digital Services Act, the Artificial Intelligence Act (AIA), and the Data Act.[3]

B. Access to justice, ADR and ODR

Alternative dispute resolution (ADR) has gained the attention of legislators and investments by developers as a faster, cheaper and easier way to solve disputes.[4] An evolution of ADR, online dispute resolution (ODR), includes all the alternative dispute resolution processes that allow the parties and

3 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) OJ L 277, 27.10.2022, 1-102; Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L, 2023/2854, 22.12.2023 and the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12.7.2024.

4 Regulation (EU) No. 524/2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No. 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR). OJ L 165, at 1, part. Recital 8. See also Schmitz, A.J. & Rule, C. (2017) The New Handshake: Online Dispute Resolution and the Future of Consumer Protection. American Bar Association.

a third party to interact at a distance using internet infrastructure. When parties find themselves in a dispute that has emerged online, they are more likely to accept online techniques to solve it and follow the internal procedure.[5] Moreover, parties appreciate the greater flexibility provided by online tools, which allows them to participate in a place and at a time that is convenient for them. Therefore, the use of the ODR process has been considered one of the tools that enhance access to justice and allow citizens to exercise their rights before a judicial court and alternative fora.[6]

It must be underlined that moving the dispute resolution process from in-person to videoconferencing by means of software applications available online may not be perceived as a substantial change that qualifies ADR as ODR. However, using such technology requires additional efforts in terms of experience and knowledge not only by the parties but, most importantly, by a potential third party involved in conflict resolution (e.g. a mediator or an arbitrator) who should master the technology to fully exploit its potential. Therefore, the technology in the ODR framework becomes a 'fourth party' that can play a proactive role and help the parties and the mediator/arbitrator to reach a fair solution.[7] Although the examples available in the market are limited and do not yet envisage all the most innovative solutions,[8] developments in ODR are already underway, and the technical and regulatory framework applicable to them will have to consider the needs of vulnerable people and the accommodation required for them.

5 See the results of a study developed in 2000 on the, at the time, first internal complaint mechanism based on mediation adopted by the e-Bay platform: Katsh, E., Rifkin, J., and Gaitenby, A., 'E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of "eBay Law"' (2000) 15 Ohio State Journal on Dispute Resolution 705.

6 This wider interpretation is also used to justify other developments of 'digital' justice such as predictive justice systems. See Longo, E. (2023) *Giustizia digitale e Costituzione*; de Souza, S. and Spohr, M. (2021) Introduction. Making Access to Justice Count: Debating the Future of Law in de Souza, S. and Spohr, M. (eds) *Technology, Innovation and Access to Justice*, 1-16.

7 Rifkin, J. (2001) 'Online Dispute Resolution: Theory and Practice of the Fourth Party' 19 Conflict Resolution Quarterly 117; Rule, C. (2002) *Online Dispute Resolution for Business: B2B, e-Commerce, Consumer, Employment, Insurance, and Other Commercial Conflicts*.

8 Loebl, Z. and Rezabkova, T. (2023) 'Forward-Looking Approach to Online Dispute Resolution (ODR) in Light of the Current and Forthcoming EU Digital Legislation' 10 International Journal of Online Dispute Resolution 42.

I. Access to justice

Access to Justice is not only a political slogan; it is a movement that arose in Western democracies in the heyday of welfarism in whatever shape in the 1960s and 1970s. In the United States, law and litigation played vital roles in the equal treatment of black people, and later in the development of collective rights to pursue common interests in courts.[9] There was a rising political awareness of the need to look after groups in society which were excluded from the blossoming economy, excluded from legal systems – perhaps not formally but in practice – and unable to defend the rights attributed to them in courts. The movement for access to justice has many facets and political and economic implications. In the US, it cannot be disconnected from the civil rights movement. In Europe, it was much more closely linked to welfarism and the growing role that states/governments were playing in setting boundaries to free market capitalism with statutory regulations to increase equal treatment and social justice.

The connection between previous research and the current political attention to the 'societally and socially excluded' has allowed socio-legal studies to develop appropriate means to integrate such categories in society. Sociology and law have been coming together in the US and Europe, at Madison, Berkely, Harvard, Yale and Stanford universities, at the Max-Planck Institute für Ausländisches und Internationales Privatrecht in Hamburg and, later at the Centre for European Legal Policy in Bremen, all of which are united in the 'Access to Justice' project run by Mauro Cappelletti at the European University Institute in Florence.[10] Research on potential barriers to courts has constituted one of the critical elements in this empirical research.

Looking at the analysis by Cappelletti on access to justice, it emerges that there have been three waves of enhancement of access to justice for citizens outside judicial proceedings, all of which can be covered by the definition of 'co-existential justice.' The first wave involved legal aid for people experiencing poverty, the second concerned enhancing public interest litigation and the third concerned the need to reform judicial systems by inviting more substance-oriented justice. In this last wave, Cappelletti's premise is

9 Handler, J. (1978) Social Movements and the Legal System: Theory of Law Reform and Social Change.

10 Cappelletti, M. and Garth, B. (1981) Access to Justice: The Newest Wave in the Worldwide Movement to Make Rights Effective, in 27 Buffalo. L. Review 181.

that some types of conflicts are more prone to 'receive' justice through alternative methods rather than through the traditional path before courts. In these cases, there is not a need to define – and eventually sanction – who is wrong and who is right, thanks to the *jus dicere* by the judge, but instead, a need to provide the means for the parties in conflict to find their own (self-determined and therefore creative) solution to the dispute. Therefore, the solution can 'mend' the relationship so that it can continue in the future. Although the idea of 'mending justice'[11] cannot be applied generally, it is more efficient when the litigation occurs as an episodic (albeit conflictual) interruption of the relationship between the parties rather than a fatal and definitive fracture. In these cases, the sword of the court's decision, which inexorably 'separates' the wrong from the right, cannot provide effective remedies. In contrast, the conflict can be overcome more effectively by creating a solution shared between the parties, allowing them to 'co-exist' while continuing the relationship.

The central insights of this research lose none of their significance when it comes to the reasons why people do not pursue their rights in court – a perception of courts as institutions that are not there to pursue the interests of the 'little people,' as is politically expressed in the formula of class justice. These countless minor barriers can be traced back to differences in education but, above all, to the barriers of domination that the judicial system itself creates – the written nature of the proceedings, the language, the distribution of roles in court and the lack of legal aid for those who cannot express themselves. There is empirical research on almost all these problems in the USA and Europe, which has not lost its relevance to the design of courts.

II. ADR in the European legal framework

Out-of-court dispute resolution has been seen as one possible way to lower the threshold to get access to justice by de-formalising the procedure, giving it a more human touch through the choice of location, the involvement of laypersons, the search for a different language and the downgrading

11 Cappelletti, M., Garth, B. and Trocker, N. (1982). Access to Justice, Variations and Continuity of a World-Wide Movement, Rabels Zeitschrift für ausländisches und internationales Privatrecht/The Rabel Journal of Comparative and International Private Law 46. Jahrg., H. 4., 664-707.

(if not exclusion) of attorneys, at least in the initial phase. Out-of-court dispute settlement, or alternative dispute settlement, covers a broad range of institutions, which vary considerably in their public or private nature, governance structure, composition, procedure, and particularly the legal effect of the decisions made in such fora, which may range across all the nuances between binding and non-binding.[12]

The rise of out-of-court dispute resolution in EU law has come together with the rise of consumer policy in the EU Member States. It started with the development of the first EC policy programmes in 1976 and 1981. It was then strengthened with the amendment of Art. 114 TFEU in 1986, which mirrored the rise, if not explosion, of EU consumer law, which was used to frame the legal completion of the envisaged internal market.[13] Although the treaty did not grant the EU the power to deal directly with law enforcement, Art. 81 TFEU sets developing judicial cooperation in civil matters with cross-border implications as one of the EU competencies. Most importantly, this includes the adoption of alternative methods of dispute settlement (part. Art. 81(2)(g) TFUE).[14]

In addition, the CJEU has generously accepted that the EU enjoys an annex competence[15] that allows it to combine the harmonisation of substantive consumer law with appropriate enforcement tools, one of which is ADR mechanisms. First, ADR was connected to the type of consumer contract. Later, a genuine European layer for outside court dispute settlements was introduced by Directive 2013/11 on consumer ADR.[16] There is no other field

12 Ortolani, P. (2021) 'Digital Dispute Resolution: Blurring the Boundaries of ADR' in DiMatteo, L. et al. (eds.), *The Cambridge Handbook of Lawyering in the Digital Age*.

13 Casarosa, F. (2023) 'The Inactive Integration Clause: Can Art. 12 TFEU Shape Future Sustainable Consumer Policies?' 7 European Papers – A Journal on Law and Integration 14311446.

14 Note that the legislative interventions on alternative dispute resolution are only one of the three sets of interventions based on Art. 81 TFEU, which include on the one hand the European small claim procedure (Regulation 861/2007) and the European payment order (Regulation 1896/2006) and on the other Directive 2008/52 on mediation. See Berto, R. (2020) 'Alternative Dispute Resolution in the Digital Sector: A Dejurisdictionalization Process?' 7 International Journal of Online Dispute Resolution 103.

15 CJEU C-359/92 Germany v. European Commission, ECLI:EU:C:1994:306 in a conflict on the enforcement tools in the directive on consumer safety.

16 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) OJ L 165, 18.6.2013, 63-79.

in EU law in which the EU legislature has devoted so much attention to developing out-of-court dispute settlement mechanisms.[17]

The consumer ADR Directive is under review: [18] the European Commission has used its reporting obligation to evaluate the Member States' ADR systems and proposed the means to improve their effectiveness, which considerably differ across the EU.[19] The proposal employs the minimum harmonisation approach, leaving broad discretion on governance to the Member States. This might contradict the expectations of consumers who favour a less heterogeneous design. The European Commission has counted 430 ADR bodies in the EU and the EEC Member States.[20] The proposed amendment has two primary objectives: the first is to downgrade the burden on companies, in particular SMEs, by reducing their reporting requirements, and the second is to broaden the scope of application, which will include individual complaints by consumers about unfair commercial practices in the digital economy. The proposed amendment must be read together with the Omnibus Directive,[21] which granted consumers

17 Compared with the very laconic interventions in Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services, in which Art. 13 requires "providers of online intermediation services and organisations and associations representing them to, individually or jointly, set up one or more organisations providing mediation services […] for the specific purpose of facilitating the out-of-court settlement of disputes with business users arising in relation to the provision of those services." Similarly, Art. 17(9) of Directive 2019/790 on copyright and related rights in the digital single market specifies that online content-sharing service providers must provide an effective and expeditious complaint and redress mechanism, which is qualified as an out-of-court redress mechanism in cases of disputes between rightsholders asking for content removal from platforms. Another example is Directive 2018/1808 amending the Audiovisual Media Services Directive, of which Art. 28b provides out-of-court redress for settling disputes between users and video-sharing platform providers.

18 Proposal for a Directive of the European Parliament and of the Council amending Directive 2013/11/EU on alternative dispute resolution for consumer disputes, and Directives (EU) 2015/2302, (EU) 2019/2161 and (EU) 2020/1828 Brussels, 17.10.2023 COM (2023) 649 final.

19 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Directive 2013/11/EU of the European Parliament and of the Council on alternative dispute resolution for consumer disputes and Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes Brussels, 17.10.2023, COM (2023) 648 final.

20 See the full list at https://ec.europa.eu/consumers/odr/main/?event=main.adr.show2.

21 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC,

individual rights under the Unfair Commercial Practices Directive 2005/29 (UCPD).[22] The proposal does not include complaints about the pre-contractual obligations of traders and does not foresee the possibility of ADR bodies bringing cases to courts if they realise that a particular legal problem needs to be clarified by the courts instead of leaving its ongoing resolution to ADR bodies.[23]

III. The notion of ODR in the European legal framework

In 2013, the EU adopted the Regulation on Online Dispute Resolution.[24] The name is misleading as the purpose was not to create an independent European ODR mechanism to directly resolve European citizens' disputes. Instead, the aim was to create a platform ('ODR platform') that lists the available (national) ADR and ODR providers. Consumers should use the platform to select and contact ADR/ODR providers and initiate a resolution procedure. According to the EU legislator, the ODR platform would facilitate independent, impartial, transparent, effective, fast and fair out-of-court resolution of online disputes between consumers and traders. The Commission was responsible for developing and operating the ODR platform,[25] including all the translation functions necessary for this regulation and its maintenance, funding and data protection. The ODR platform was to be a multilingual interactive website allowing consumers to contact

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 (Text with EEA relevance) OJ L 328, 18.12.2019, 7-28.

22 Directive 2005/29/EC of the European Parliament and of the Council 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') (Text with EEA relevance), OJ L 149, 11.6.2005, 22–39.

23 BEUC Report, Modernising Consumer ADR in the EU. The revision of Directive 2013/11/EU on consumer Alternative Dispute Resolution, 15 December 2023 https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-164_Modernising_Consumer_ADR_in_the_EU.pdf.

24 Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) OJ L 165, 18.6.2013, 1–12.

25 https://ec.europa.eu/consumers/odr/main/?event=main.home2.show.

traders to open an ADR procedure online. The ODR platform was regarded as a complement to the blossoming online business. The EU made great strides in the online platform and above all in handling cross-border conflicts. The Consumer Advice Centres, which the EU set up and financed for this purpose, were intended to play a unique role.[26] However, the project did not fly. This is why insiders were not surprised when the 2019 review of the ODR Regulation revealed its somewhat limited importance.[27] Despite a high number of visits, there was limited consumer interest in requesting an ADR procedure from the traders concerned, who, in most cases, either remained silent or offered to settle the case outside of the platform. As a result, about 2% of the requests for an ADR process were sent to an ADR entity. The situation has not improved, as the 2023 report demonstrates.[28]

In its proposal to withdraw the ODR Regulation,[29] the European Commission explains:

> Once a request is made by the consumer, the trader has 30 days to agree to launch the ADR process. Only 2% agree to do so, about 40% of the traders contact the consumers directly outside the platform to settle the matter while the majority of traders simply remain silent as participation is not compulsory. ADR bodies perform a test of eligibility on the cases reaching them (about 400 per year) and on average keep only half of the requests. The poor results of the ODR platform are therefore the result of a succession of facts linked to the lack of prior information of visitors on how ADR works, the very limited interest of traders and the

26 https://www.eccnet.eu/consumer-rights/exercising-your-consumer-rights/online-dispute-resolution-platform.

27 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Directive 2013/11/EU of the European Parliament and of the Council on alternative dispute resolution for consumer disputes and Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes, COM(2019) 425 final.

28 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Directive 2013/11/EU of the European Parliament and of the Council on alternative dispute resolution for consumer disputes and Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes Brussels, 17.10.2023, COM (2023) 648 final, 7.

29 Proposal for a Regulation of the European Parliament and of the Council repealing Regulation (EU) No 524/2013 and amending Regulations (EU) 2017/2394 and (EU) 2018/1724 with regard to the discontinuation of the European ODR Platform, COM/2023/647 final.

uneven completeness or relevance of the consumer complaints about the eligibility criteria set by ADR entities.

If we compare these results with the statistics available for the European market, the results are not that different, but the importance of ADR/ODR is still far-reaching.[30] This is not because there are few disputes occurring in the online context but instead the opposite, as at least a quarter of the 71.2% of citizens who have purchased goods and services online have experienced problems regarding such purchases. However, only two-thirds have decided to react, and among the available options for redress selected ADR in 6.2% of the cases. Although this is a low percentage, it is still the second option after complaining before a public authority.[31] It is interesting to verify the reasons for this lack of reaction, as they may indicate the problems citizens encounter when deciding to pursue a claim concerning an online purchase. The problems acknowledged include not only the well-known challenges, namely the length of the procedure and the fact that the sums involved were small. The lack of knowledge regarding the complaint mechanisms available also reveals that the process would be too complex or would require filling in many documents or using complicated language. This last element is perceived as a barrier for 24.9% of the citizens who decided not to exercise their rights. This element reveals one of the more problematic aspects of achieving access to justice: when looking at the advantages of digitalisation, the benchmark used is the average online user, who is not only able to reap the benefits of digital markets, i.e. buying goods or services online, but is also able to exercise their rights when a violation occurs, if necessary in English as a lingua franca. Limited or no attention is given to online users with less knowledge or less confidence to exercise their rights.[32]

On the same day, together with the proposal to amend the ADR Directive and withdraw the ODR regulation, the European Commission adopted a

30 See the results of the 2022 Consumer conditions survey – standard survey, available at https://commission.europa.eu/document/download/0cdcc170-e877-4b3b-b4eb-404f47596896_en?filename=Consumer%20Conditions%20Survey%20-%20standard%20survey.xlsx.

31 Note that the first option selected by (81% of) the users is to complain about the retailer or service provider (or manufacturer). However, this is a preliminary step that in the case of dissatisfaction may lead to selecting a conflict resolution path.

32 This problem has already been acknowledged. See Schmitz, A.J. (2012), Access to Consumer Remedies in the Squeaky Wheel System.

recommendation on quality requirements for dispute resolution procedures offered by online marketplaces and Union trade associations.[33] The recommendation addresses in-house complaint-handling procedures between businesses and consumers and defines some basic expertise, independence, impartiality, effectiveness and fairness requirements. It reads like a slim version of the proposed amended ADR Directive, which it refers to throughout the text. In this sense, the recommendation is to be regarded as the functional equivalent of Art. 20 of the Digital Services Act (DSA), which lays down the mandatory requirement "*to lodge complaints, electronically and free of charge, against the decision taken by the provider of the online platform upon the receipt of a notice or against the following decisions (listed in Art. 20 (1) a)-d)) taken by the provider of the online platform because the information provided by the recipients constitutes illegal content or is incompatible with its terms and conditions*."[34]

The choice of a recommendation brings back a memory of the predecessors of the ADR Directive, namely the two Recommendations 98/257 and 2001/310.[35] Here, the CJEU gave the recommendations legal weight by turning the non-binding recommendations into quasi-binding law.[36]

33 Commission Recommendation (EU) 2023/2211 of 17 October 2023 on quality requirements for dispute resolution procedures offered by online marketplaces and Union trade associations (notified under document C/2023/7019, OJ L, 2023/2211, 19.10.2023.

34 According to Art. 3 b) DSA, "'*recipient of the service*' *means any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible*." The definition includes consumers in the variety of interactions they initiate with online platforms or search engines. These are tied to a particular activity – information seeking or information supply, provided the activity reaches beyond information seeking and providing they become 'active recipients' in the meaning of Art 3 (p) and (q), which again encompasses the consumer. Content moderation includes the guarantee of a "*high level of consumer protection in Art. 38 of the Charter* (Art. 34 (1) b) DSA)" more generally and the interests of children/minors and handicapped people more specifically (Art. 34 (1) b) and d) DSA). For a detailed analysis, see Micklitz, H.-W. (2024), The Dissolution of the EU Consumer Law Acquis through Fragmentation and Privatisation, forthcoming.

35 See Commission Recommendation 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes, OJ L 115, 17 April 1998, 31 and Commission Recommendation of 4 April 2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes, C(2001) 1016, OJ L 109, 19 April 2001, 56.

36 CJEU Case C-317/08 Alassini, ECLI:EU:C:2010:14.

C. Regulation of vulnerabilities in the industrial economy

The rise of national, EU and worldwide consumer law is inherently connected to the understanding that consumers need protection, that they are weaker than businesses, and that regulatory means are necessary to compensate for the imbalance of power and information asymmetry. There was previously no distinction between the different classes of consumers, as all consumers were perceived as being in a weaker position vis-à-vis professionals and traders. In the 1970s and 1980s, speaking of a 'weak consumer' would have been a pleonasm. The wind turned with the EU taking over consumer protection after the Single European Act. The previous "consumer protection law" gradually became a "consumer law without protection."[37] In the CJEU's case law, understanding national advertising laws as restricting market freedoms was the game changer. The Court developed the concept of the average consumer – an informed, circumspect and responsible consumer – as the one against which national advertising laws had to be balanced. This yardstick allowed the CJEU to eliminate national advertising laws to protect SMEs against new upcoming marketing strategies in the name of consumer protection.[38] This does not mean the CJEU used the same yardstick outside the legal context. The average consumer in advertising law has to be delineated from the weak consumer to whom the CJEU refers when monitoring unfair terms.[39]

The last two decades have seen a revival of the weak consumer as opposed to the average one, now redefined with the more neutral definition of *vulnerable* consumer. This development is gaining pace at the EU and Member State levels, but not only there.[40] The vulnerability concept is often used to identify users or groups of users that require regulatory/policy attention because of their lack of bargaining power, structural inequalities

37 Micklitz, H.-W. (2012), The Expulsion of the Concept of Protection from the Consumer Law and the Return of Social Elements in the Civil Law. A Bittersweet Polemic. 35 Journal of Consumer Policy 283-296.

38 Unberath, H. and Johnston, A. (2007), 'The double-headed approach of the ECJ concerning consumer protection. 44 Common Market Law Review 1237-1284.

39 Ginestri, M. (2023), Equality of Superiority of the Weak Party? Consumer Protection and the Issues at Stake, ECRL 375; Micklitz, H.-W. and Reich, N. (2014), The Court and Sleeping Beauty: The revival of the Unfair Contract Terms Directive (UCTD). 51 Common Market Law Review 771-808.

40 N Helberger et al. (2022) 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' 45 Journal of Consumer Policy 175.

and other market or social conditions that make them more susceptible to harm, for example, in the form of discrimination or unequal treatment. At times it is also used as a concept to allow differentiation in situations in which uniform treatment of all would lead to unfairness for some. Peroni and Timmers show that, in the case law of the European Court of Human Rights, acknowledgement of the vulnerability status of particular groups, such as Roma, people with mental disabilities, people living with HIV and asylum seekers, led the ECtHR to find special positive obligations on the part of the state, increase the weight of harm in proportionality analysis and reduce states' margin of appreciation.[41] Malgieri and Niklas also trace the development of vulnerability as a concept in data protection law.[42] In this legal area, however, the concept has mostly been confined to the protection of minors, who are less aware of the potential risks and consequences of data protection and who, therefore, warrant a higher level of protection concerning the right to transparency, profiling, and informed consent.[43]

Seen through the lens of consumer policy, three different strands are coming together, and they are described in the following paragraphs.

I. Vulnerabilities in universal service obligations

The first strand addresses liberalisation, and partly privatisation, of formerly state-owned finance, telecom (today electronic communication), energy and transport companies, which has made it necessary to distinguish between 'customers' who can pay the market price and those who cannot. The latter need access at an affordable price. So far, there is not much clarity on what an affordable price means and what exactly has to be done to fight energy poverty, grant everybody access to an affordable bank account and provide affordable prices in public transport and electronic communication. The uncertainty is increased by a debate on what exactly belongs

41 Peroni, L. and Timmer, A. (2013). Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law. International Journal of Constitutional Law 11 (4): 1056-85. See also Chapman, A. and Carbonetti, B. (2011), Human Rights Protections for Vulnerable and Disadvantaged Groups: The Contributions of the UN Committee on Economic, Social and Cultural Rights. Human Rights Quarterly 33 (3): 682-732.

42 Malgieri, G. and Niklas, J. (2020), Vulnerable Data Subjects. Computer Law & Security Review 37: 10541.

43 Recitals 38, 58, 65 and 75 GDPR.

to universal services.[44] Here, vulnerability focuses on a lack of economic resources.

II. Vulnerabilities in the UCPD

The second strand results from the harmonisation of unfair commercial practice law in the UCPD, as agreement on a full harmonisation approach could only be reached once the notion of the average consumer was complemented with the newly introduced vulnerable consumer in Art. 5 (3).[45] Protection is limited to a "clearly defined group" (sic!) who are vulnerable due to their "*mental or physical infirmity, age or credulity.*" Legal scholarship has spent much ink on concretising the four categories.[46] As a rule, commercial practices must be assessed from the perspective of the average consumer, the prototype of the European consumer, who is "reasonably well-informed and reasonably observant and circumspect," as defined in Recital 18 UCPD. It is the perspective of the average consumer that is relevant when assessing the fairness of a particular practice. Art. 5 (3) defines the exception to the rule.[47] However, Art. 5 (3) has not gained much importance in practice, maybe because of the barriers to identifying the group. The EC Guidance on Interpretation of the UCPD demonstrates the lack of case law. Member State courts and the CJEU are seeking a solution to lower the average consumer standard.[48] Outside the field of

44 Bartl, M. (2010), The Affordability of Energy: How much protection for the vulnerable consumer? 33 Journal of Consumer Policy 225-245; Johnston, A. (2016), Seeking the EU 'Consumer' in Services of General Economic Interest, in D. Leczykiewicz and St. Weatherill (eds.), The Images of the Consumer in EU Law. Legislation, Free Movement and Competition Law., 93-138.

45 Wilhelmsson, T. (2006), Chapter 3 Scope of the Directive, in Howells, G., Micklitz, H.-W. and Wilhelmsson, T. European Fair Trading Law. The Unfair Commercial Practices Directive, 49.

46 Leczykiewicz D. and Weatherill S. (eds.) (2016), The Images of the Consumer in EU Law. Legislation, Free Movement and Competition Law; Casarosa, F. (2020) The Rights of People with Disabilities in EU Consumer Law in D. Ferri and A. Broderick (eds.), Research Handbook on EU Disability Law.

47 Concerning the UCPD, this is common sense. Peroni and Timmer (2013, 1061) show that a similar dichotomy characterises the dominant stance in the treatment of vulnerability in human rights law.

48 Schebesta, H. and Purnhagen, K.P. (2016), The Behaviour of the Average Consumer: A Little Less Normativity and a Little More Reality in the Court's Case Law? Reflections on Teekanne (6 June 2016). 41 European Law Review 590.

unfair commercial practices in the core area of consumer contract law, the notion of the vulnerable consumer did not gain much ground when the consumer acquis was revised along the lines of the consumer REFIT programme. Only timid efforts were made to re-introduce the vulnerable consumer in the EU consumer contract acquis. An example is Recital 34 of the Consumer Rights Directive,[49] which obliges traders to take the different capacities of consumers to process information into account. It is worth quoting:

> *The trader should give the consumer clear and comprehensible information before the consumer is bound by a distance or off-premises contract, a contract other than a distance or an off-premises contract, or any corresponding offer. In providing that information, the trader should consider the specific needs of consumers who are particularly vulnerable because of their mental, physical or psychological infirmity, age or credulity in a way that the trader could reasonably be expected to foresee. However, considering such specific needs should not lead to different levels of consumer protection.*

The recital demonstrates the ambiguity of the legislation. How should it be possible to distinguish between the average and the vulnerable consumer without imposing a different level of protection? The distinction between the two implies what the recital wants to exclude. This might explain why the recital is still waiting to be awakened to life by the enforcement authorities and maybe even national legislatures.[50] In consumer policy and research, there is vibrant discussion on the potential need to revise the average consumer benchmark and shape the vulnerable consumer concept.[51]

---

49 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, Text with EEA relevance. OJ L 304, 22.11.2011, 64-88.

50 Sachverständigenrat für Verbraucherfragen, Personalisierte Verbraucherinformation: Ein Werkstattbericht, Dokumentation einer Veranstaltung des SVRV, Veröffentlichungen des Sachverständigenrats für Verbraucherfragen, 2022, https://www.conpolicy.de/aktuell/personalisierte-verbraucherinformation-ein-werkstattbericht.

51 Grochowski, M. (2021), Does European contract law need a new concept of vulnerability? 4 EuCML 133.

III. Vulnerabilities in ADR and ODR

The consumer ADR Directive and the ODR Regulation were adopted in 2013 when vulnerability in universal services and commercial practices had long become an issue in political discourse. Therefore, one might have expected that both EU measures address vulnerabilities. However, the consumer ADR Directive does not mention vulnerabilities at all. In contrast, Art. 5 ODR Regulation addresses the European Commission: "*The development, operation and maintenance of the ODR platform shall ensure that the privacy of its users is respected from the design stage ('privacy by design') and that the ODR platform is accessible and usable by all, including vulnerable users ('design for all'), as far as possible*." Who the vulnerable users are, however, is nowhere defined.

The 17 October 2023 proposal to amend the ADR Directive looks more promising as it refers to barriers resulting from digital literacy and barriers other than language.

> Recital (2): There are additional barriers in cross-border ADR, like language, lack of knowledge of the applicable law, and specific access difficulties for vulnerable consumers.
> Recital (10): Member States should ensure that ADR enables consumers to initiate and follow ADR procedures offline if requested. It should also be ensured that when digital tools are provided, they can be used by all consumers, including vulnerable consumers or those with varying levels of digital literacy. Members States should ensure that, upon request, parties to the disputes always have access to a review of automated procedures by a natural person.

The recitals, however, have been watered down in the proposed revision of Art. 5 (2) ADR. The language remains vague and leaves much room for interpretation if not for disregarding vulnerabilities.

> "(a) ensure that consumers can submit complaints and the requisite supporting documents online in a traceable manner and ensure that consumers may also submit and access these documents in a non-digital format upon request;
> (b) offer digital ADR procedures through easily accessible and inclusive tools;"

It remains to be seen whether and to what extent the current proposal will undergo revision in the ongoing trialogue.

D. Regulation of vulnerabilities in the digital economy

The third strand is deeply connected to EU digital policy legislation. While the various regulations, particularly the AIA, the DSA and the Data Act, heavily affect consumers as defined in the EU consumer law acquis, neither regulation explicitly addresses consumers and their rights. The horizontal character of the regulations, which concern the digital economy and digital society, might nevertheless explain why already well-known vulnerabilities in the two previous strands of development are now mixed up with discriminatory practices and vulnerabilities of disabled people and minors.[52] One might therefore break down vulnerabilities in the EU digital policy legislation into the *societally discriminated* – those who come under the EU non-discrimination law acquis, the *economically discriminated* – those who are potential customers of universal services (although it is unclear whether and to what extent the proposal of the EP will make it into the official version) and *disabled persons* and *children/minors.* [53]

I. Vulnerabilities in the AIA, the DSA and the Data Act

The AIA and the DSA stress the risk of being discriminated against and the critical role of the right not to be discriminated against in the EU Charter of Fundamental Rights (EU Charter), but without going into detail about the various forms of prohibited discriminatory practices and how they might affect the various groups mentioned in the EU non-discrimination law acquis. The emphasis is on eliminating discriminatory practices, not specifying the vulnerabilities of the people affected. Economic vulnerability remains equally underdefined. The Data Act instead repeatedly refers to non-discriminatory and fair behaviour. However, it applies in the context of contractual agreements with parties with different market powers, showing that imbalances among traders can result in a need for additional monitoring.

52 This contribution refers to the provisional agreement resulting from interinstitutional negotiations: Proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021/0106(COD), 2 February 2024.

53 Micklitz, H.-W. (2018), The Politics of Justice in European Private Law.

International standards seem to be more detailed. ISO Standard 22458:2022 on consumer vulnerability and providing requirements and guidelines for the design and delivery of inclusive service is the only document pointing to some concept.[54] The ISO approach is to be taken as a serious effort to conceptualise 'vulnerability' very differently and far more forward-looking than the EU legislation, be it the consumer acquis or the digital policy legislation. Two constitutive elements of the ISO concept of vulnerability are worth highlighting. First, vulnerability is regarded as an individual personal characteristic – everybody can be vulnerable; the second is the broad set of impact factors which may trigger vulnerability: they can be (1) *personal* factors resulting from limitations in individual capacities; (2) *situational* factors resulting from managing information, getting access to or choosing suitable services, having difficulties in making decisions in one's best interests, understanding one's particular rights or pursuing one's rights, or (3) factors coming from the *market environment* – a criterion which is mentioned but seems relatively underdeveloped at least in the previously mentioned EU legislation. These explanations and interpretations are then translated into a definition of consumer vulnerability and vulnerable situations, which can be temporary, sporadic or permanent.[55] The distinction between these three vulnerability indicators: personal, situational and market environment seems promising.

The AIA and the DSA devote particular attention to concretising the potential vulnerabilities of people with disabilities and children/minors. Both regulations explicitly refer to the UN Convention on the Rights of Persons with Disabilities (CRPD), but without imposing a binding obligation on providers and deployers to design the AI system in line with the rights concretised in the UNCRPD and later in Directives 2016/2102[56] and 2019/882.[57] Instead, the approach adopted in the DSA looks like a blueprint for the AIA. Recital 105 DSA sets the tone for the level of regulatory intervention: non-binding action. However, not even online platforms are addressed; they are only very large platforms and search engines. Art. 47

54 https://www.iso.org/standard/73261.html.

55 https://www.iso.org/obp/ui/en/#iso:std:iso:22458:ed-1:v1:en.

56 Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies, OJ L 327, 2.12.2016, 1.

57 Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services, OJ L 151, 7.6.2019, 70-115, European Accessibility Act.

DSA details how a code of conduct to increase the accessibility, inter alia, of persons with disabilities should look. The AIA postpones protection by design to the future. Recital 142 requires the Member States to promote research "*including but not limited to development of AI-based solutions to increase accessibility for persons with disabilities [and] tackle socioeconomic inequalities*". [58] The only concrete measure increasing the protection of persons with disabilities is in the minimum criteria the codes of conduct must meet. Art. 95 refers to "*assessing and preventing the negative impact of AI systems on vulnerable persons or groups of persons, including accessibility for persons with a disability, as well as on gender equality.*"

The second category is children/minors. Art. 1 CRPD defines every human being below the age of eighteen as a child.[59] EU law does not have a definition of minors or children, not even in Art. 24 of the EU Charter. It does not even use the word 'minors.' However, neither the AIA nor the DSA closes the definitional gap with reference to the CRPD. Where the CRPD is mentioned, both acts speak of the rights mentioned, deliberately avoiding clarification.[60]

Throughout the text, the DSA mentions the need to protect minors in the platform economy. The website where the EU presents the DSA devotes a paragraph to the envisaged "strong protection of minors." The language sounds like marketing: "*platforms will have to redesign their systems to ensure a high level of privacy, security, and safety of minors; targeted advertising based on profiling towards children is no longer permitted; special risk assessments including for negative effects on mental health will have to be provided to the Commission 4 months after designation and made public at*

58 It is interesting to note that the amendments presented by the European Parliament were not included in the final text. The proposed text of Art. 84 on the evaluation and review of AIA included the "the effect of AI systems on health and safety, fundamental rights, the environment, equality, and accessibility for persons with disabilities (emphasis added), democracy and the rule of law and in the light of the state of progress in the information society."

59 Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 and entered into force on 2 September 1990, in accordance with Art. 49, https://www.ohchr.org/sites/default/files/crc.pdf.

60 See Art. 9 AIA. Also in this case, the amendments of the European Parliament were disregarded. Art. 52 b) (3) AIA-EP required that AI providers and deployers should consider children's information capabilities when drafting the transparency requirements. Similar amendments concerned the minimum criteria codes of conduct must meet.

the latest a year later; platforms will have to redesign their services, including their interfaces, recommender systems, terms and conditions, to mitigate these risks."[61] The prohibition on profiling children for marketing purposes is by far the most critical ruling.

The many references to 'minors,' not to children, in particular in the recitals, unfold an impressive language on the comprehensibility of terms and conditions (recital 46), on an appropriate design of the interface (recitals 71 and 81), on accessibility of notice and action, on complaint mechanisms (recital 89) and on content impairing their physical, mental or moral development (recital 89). These overall purposes are reflected in two provisions. Art. 14 of the DSA on terms and conditions introduces a ruling that opens a new page in the control of standard terms, which raises the question of the interaction between the DSA and the Unfair Contractual Terms Directive (UCTD). One may understand Art. 14 DSA as an integral part of the transparency requirement in Art. 4 UCTD, which would imply that consumer agencies and consumer organisations enjoy standing, a reading which is indirectly supported by the integration of the DSA in the Annex of Directive 1828/2018 on Representative Action,[62] pursuant to Art. 90 DSA. In addition, DSA Art. 28 is devoted to the "online protection of minors." The high level of privacy, safety and security in connection with the recitals calls for an appropriate algorithmic design. Again, the question arises of how to qualify this obligation. Is it an obligation to unfold effects between platforms and consumers/minors or only between platforms and enforcement authorities? In the first variant, Art. 28 (1) DSA may be integrated in the broad concepts of transparency and fairness in the UCTD. These somewhat promising tendencies in Articles 14 and 28 DSA are thwarted when confronted with how the DSA seeks a solution to promote the rather ambitiously worded protection of minors. Recital 102 and Art. 44 DSA deal with "standards," which are all voluntary, not semi-binding harmonised European standards. The protection of minors is reduced to the least stringent regulatory measure: voluntary standards.

Art. 34 (1) b) DSA requires respect for children's rights, as is enshrined in Art. 24 of the EU Charter, and a high level of consumer protection, as is enshrined in Art. 38 of the EU Charter. One might have expected that

61 Website of the European Union: https://www.eu-digital-services-act.com.

62 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ L 409, 4.12.2020, at 1.

the EU legislature would have imposed clear obligations on what platforms would have to do, not least in the light of the experience of monitoring and surveillance of TikTok.[63] In its assessment, the European Commission regards the different safeguards enshrined in the DSA as a significant success.[64]

This is not all. The EU digital policy legislation refers to vulnerabilities of AI systems, conquering the concept and giving it a twist, which points in a very different direction, away from personal vulnerability for whatever reason to system vulnerability, to the risk of cyber-attacks and the like (recital 76 AIA). The parallel with the European Convention on Human Rights springs to mind when plaintiffs – businesses and citizens/consumers – discovered the potential to turn economic rights into human rights.[65] In sum, there does not seem to be a clear perspective underpinning the AIA and the DSA. The term is used randomly, perhaps with an inclination to equate vulnerabilities with societal discrimination. There is an urgent need to conceptualise vulnerability, a task that goes beyond the scope of this contribution. [66]

II. Dispute resolution in the AIA, the DSA and the Data Act

The AIA, does not contain rules on complaint handling and dispute resolution, unlike the DSA, which deals with both, and the Data Act, which at least addresses dispute resolution. The strange mismatch between mandatory requirements on complaint handling in the scope of the DSA and non-

63 Cantero Gamito, M. and Micklitz, H.-W. (2023), Too much or too little? Assessing the Consumer Protection Cooperation (CPC) Network in the protection of consumers and children on TikTok. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf.

64 See the stocktaking in Brussels, 11.5.2022 COM(2022) 212 final, A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN.

65 Abrisketa, J. and Churruca, C. , de la Cruz, C., García, L., Márquez, C., Morondo, D., Nagore, M., Sosa, L. and Timmer, A. (2015), Human rights priorities in the European Union's external and internal policies: an assessment of consistency with a special focus on vulnerable groups, European Commission.

66 Malgieri, G. (2023) 'The Notion of the Data Subject: An Average Individual?' in Gianclaudio Malgieri, *Vulnerability and Data Protection Law*.

binding Recommendation 2023/2211 has already been addressed.[67] What remains to be analysed is the relationship between the consumer ADR Directive, together with the proposed revisions and the rules on dispute resolution in Art. 21 DSA. In its proposal, the European Commission starts with the compatibility of the two,[68] affirming that

> Art. 21 Digital Services Act on out-of-court dispute settlement is without prejudice to the ADR Directive (Art. 21(9)). Furthermore, it regulates how users of intermediary services can complain about the intermediary's content moderation decisions about illegal or harmful content, including where the service provider decides not to take action following a notice. Even if such illegal content or content that is otherwise incompatible with the intermediary terms and conditions may concern a third-party trader's bad commercial practices, the dispute pursuant to Art. 21 DSA will be settled between the intermediary and the recipient concerned by the content moderation decision and is limited to the restrictions applicable to the content or account in question. The ADR Directive will remain applicable for consumer disputes with the third-party trader that generally concern how to get money back, how to get a faulty product repaired, how to stop a contract that was based on unfair terms, etc.

According to the Commission, the consumer ADR Directive provides for dispute resolution addressing illegal commercial practices by traders, which is complementary to that provided for disputes addressing content moderation performed by intermediaries. The implications of such a formalistic understanding are far-reaching. A consumer who complains about content moderation may use the dispute settlement procedure in Art. 21 DSA; the same consumer who complains about deficiencies in the online sales transaction is referred to in the revised ADR Directive. Seen through the lens of the EU approach, the distinction sounds self-explanatory. Turning the perspective upside down, seen through the lens of a – vulnerable – consumer, the differentiation looks like a deterrent to the prosecution of consumer rights.

67 See Under II.3.

68 See at page 5 of the Explanatory Memorandum to the Proposal for a Directive of the European Parliament and of the Council amending Directive 2013/11/EU on alternative dispute resolution for consumer disputes, and Directives (EU) 2015/2302, (EU) 2019/2161 and (EU) 2020/1828 Brussels, 17.10.2023 COM (2023) 649 final.

Moreover, Art. 21 (3) DSA requires a different certification mechanism than that in the revised consumer ADR directive. The latter relies on each Member State deciding to set up a system to certify the ADR bodies in the DSA. The EU legislator is more detailed and explicitly asks for the list of requirements defined in the regulation to be evaluated by the Digital Services Coordinator of the Member State in which the out-of-court dispute settlement body is established.[69] However, the certification mechanism in the DSA is incomplete. It lacks any additional specification regarding the definition of applicable standards, the type of evaluation, the geographical scope of the certification scheme and the duration of the certification appraisal. This is a lost opportunity that a lack of knowledge or expertise cannot justify, as in many other legislative interventions, the Commission has engaged in a more structured description of the certification mechanism.[70] Generally, a certification scheme should involve at least two phases: a conformity assessment and an attestation of conformity, the latter being a statement that the underlying process, product or person complies with a set of pre-defined requirements based on the objectives and scope of each certification scheme. A detailed description of the procedure is absent in the DSA. On the one hand, the legislation relies on the resources and expertise of the digital services coordinator at the national level. Art. 39 DSA provides a safety net. The provision acknowledges that digital services coordinators should carry out their tasks independently and that the Member States should ensure that they have adequate technical, financial and human resources. On the other hand, nothing is stated about the powers of the body regarding evaluating certification schemes. There is no help in Art. 41 DSA. No mention is made of the supervision, investigation and sanctioning powers of out-of-court dispute settlement bodies.

Other interesting elements are the validity of certifications and their geographical scope. The out-of-court dispute settlement body can only be certified in the country in which it is established. Although Art. 21(3) DSA acknowledges that the out-of-court dispute settlement body can provide its services in other EU languages, it does not expressly state whether the certification should be recognised in other countries. This is an evident lack

69 The Digital Service Coordinator is defined in Art. 49 DSA as the national authority with the competence to verify the application and enforcement of the DSA in each Member State.

70 Casarosa, F. (2023) 'Out-of-Court Dispute Settlement Mechanisms for Failures in Content Moderation' 14 JIPITEC, http://www.jipitec.eu/issues/jipitec-14-3-2023/5844.

of foresight as the attestation of conformity provided by the certifying body should allow services to be provided across Europe. It will be difficult for an out-of-court dispute settlement body to only provide its services in one country. Instead, it will aim to specialise in disputes emerging on certain platforms to provide service to users regardless of their nationality and language.

The dispute resolution in Art. 10 of the Data Act follows the DSA. It has similar requirements for the certification of the potential dispute settlement bodies. However, it does not allocate the certification task to a specific authority as the DSA does; instead, it refers in general to Member States. In this case, more leeway for the organisation of the certification procedure is provided, yet this can trigger greater differences at the national level. This approach can be understood if we acknowledge that the cases to be solved by the dispute resolution bodies are at the intersection between data protection and contract law, and most probably between traders who are interested in accessing data to develop novel digital products. Therefore, neither the consumer nor the data protection authority would have the comprehensive knowledge and expertise to set up such a certification scheme.

One additional element that emerges from the DSA concerns the reporting obligations to ensure compliance with the transparency requirement in Art. 24 DSA. As mentioned above, Art. 17 DSA requires all hosting service providers to inform users whenever they remove or otherwise restrict access to their content (statement of reason). Then, according to Art. 24 (5) DSA, providers of online platforms send all their statements of reasons to the Commission's DSA Transparency Database for collection.[71] Given that the number of decisions has already surpassed three million, it is reasonable to think that online platforms will adapt their statements to the technical requirements that must be met for the transparency database. In other words, the API (application programming interface) set up by the Commission in the transparency database may affect both the structure and the content of decisions by the online platform. Given that the same obligation is applicable to dispute settlement providers, pursuant to Art. 21 (4) DSA,[72] the type of data that digital services coordinators will require may

71 The DSA transparency database is available at https://transparency.dsa.ec.europa.eu/.

72 The dispute settlement provider should report annually to the digital services coordinator on their functioning, specifying at least the number of disputes it received,

affect the content and the structure of decisions by the dispute settlement provider.

III. The EC digital fairness initiative

Since the launch of the various draft regulations in the summer of 2020, consumer advocates have criticised the European Commission for downplaying possible tension between the consumer law acquis and the EU digital policy legislation and for neglecting the need to study the potential impact of the digital economy on consumers more particularly to find out whether and to what extent the current consumer law acquis provides an adequate level of consumer protection.[73] Under intense pressure from consumer advocates, which gained support from the European Parliament, the European Commission launched the Digital Fairness Fitness Check in spring 2022.[74] The evaluation will look at the UCPD, the Consumer Rights Directive 2011/83/EU and the UCTD to determine whether they ensure a high level of protection in the digital environment. In the envisaged schedule, the Commission is expected to provide a report before the closure of the current term which will concretise the direction in which the European Commission intends to go after the election in June 2024 and after the European Commission and the European Parliament have been re-established. The report is expected to be published in the second quarter of 2024.

The EC initiative triggered a debate in academic studies on what needs to be done to adapt the consumer law acquis. It is commonly agreed that the scope is too narrow as it excludes the GDPR, and more generally law enforcement, individually or collectively, in courts or with ADR and ODR mechanisms. 'Digital vulnerabilities' are centre stage. One of the authors was involved in preparing the Consumer Law 2.0. The study was commissioned by BEUC and published in 2021.[75] The report argues that digital vulnerability is structural, architectural and relational. Below is a summary

information about the outcomes of these disputes, the average time taken to resolve them and any shortcomings or difficulties encountered, pursuant Art. 21(4) DSA.

73 See the BEUC website and the various reports BEUC published on the DMA, the DSA, the AIA etc. and the various reports by national consumer organisations.

74 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en.

75 Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M. and Strycharz, J. (2021), EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets, a

of the arguments in the form of recitals for a potential amendment to the UCPD.

(1) Digital vulnerability can be condensed in the distinction between the external structural impact on consumers and their internal dispositional capabilities to make informed autonomous decisions regarding commercial practices that use digital strategies such as profiling, data-driven targeting and the design of defaults in digital choice environments. The external structural impact covers the digitally mediated relationship, the chosen architecture, the technical infrastructure of a digital marketplace, data collection, the trust relationship that consumers build with the provider of the chosen architecture over time and information asymmetries. All these have in common that they are external to the consumer in that they result from how technology is used and applied. Each consumer is confronted with the external structural impact and is therefore dispositionally vulnerable. Internal dispositional vulnerability refers to variations in individual capacities to make informed and autonomous choices in the external structure. They may be situational, informational, or source-bound.

(2) The distinction between external-structural and internal-situation impact needs to be integrated in the conceptual and regulatory toolbox. Non-legal literature uses the notion of 'digital vulnerability.' In the consumer law acquis, vulnerability is a loaded term, like weakness. This is why the legal concept has to do justice to both dimensions of digital vulnerability, the external-structural and the internal-dispositional ones. The notion of digital asymmetry avoids those pitfalls and emphasises the structure and architecture of data exploitation strategies, thereby leaving room for the internal situational impact. Regulatory attention should move towards tackling the sources of digital vulnerability, as is enshrined in the formula of digital asymmetry.

(3) The consumer's capacity to make autonomous decisions in data-driven commercial choice environments cannot be properly addressed if ensuring consumer autonomy is only understood as a) preventing direct interference with the mental/deliberative processes of consumers at the precise moment they make a transactional decision, b) ensuring the formal availability of different choices and c) being limited to the act

joint report from research conducted under the EUCP 2.0 project, BEUC, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf.

of buying and selling itself. Ensuring consumer autonomy in the digital economy requires a wider understanding of what true autonomous decision-making entails and also of a transactional decision. Consumers are not only paying with money; they are also paying with their data and their relational commitment.

(4) To ensure consumer autonomy in the digital economy, more attention needs to be paid to the difference between the formal availability of alternative choices and the material circumstances that enable consumers to actually see, understand, and exercise their capacity to make different choices. In this context, moreover, special attention should be given to the fact that data-driven commercial services try to build ongoing commercial relationships with consumers. The (personal) user data that are collected over time put the trader in a position of power to understand the behavioural patterns of users and their cognitive and behavioural biases and tendencies. This position of power can be used to subtly 'shape' consumers' preferences, motivations and behaviour more generally over time in the interests of traders without benefiting consumers or even harming consumers' true informed interests. Because such processes happen over time, they do not always constitute *direct* interference with the decision-making capacities of consumers and they do not always formally remove choice options. Nevertheless, such data-driven commercial practices can threaten consumer autonomy in the wider sense outlined here if they indirectly interfere with consumers' autonomous choices.

(5) Situations in which data-driven commercial environments use their position of power to build ongoing commercial relationships with users and keep consumers tied to their platform or service can in certain circumstances constitute situational monopolies. Situational monopolies can undermine consumers' capacity for autonomous decision-making and the exercise of free choice. Similarly, data-driven commercial environments that engage in algorithmic manipulation should be understood as undermining consumers' capacity for autonomous decision-making. 'Algorithmic manipulation' should be understood as a hidden use of data-driven targeting strategies, personalisation strategies or any other type of strategy which is aimed at influencing the autonomous decisions of consumers in ways that primarily benefit the trader, for example by identifying personal or population characteristics or circumstances that can be leveraged to increase the chances of changing the behaviour of consumers.

The potential consequence would be to reverse the burden of proof to the benefit of consumers.[76] Another proposal, which has been promoted by B.B. Duivenvoorde,[77] aims to merge the average and vulnerable consumer in the UCPD into a new concept that would *de facto* and *de jure* lead to a revision of the average consumer standard. The same author proposes introducing a new article on 'manipulation' to deal with what the author of the BEUC study calls digital vulnerability.

E. Challenges for further research

Given that statistics show that it is not uncommon for online users to feel less confident about exercising their rights, efforts should be made to introduce accommodations to enhance access to justice for vulnerable people. However, in the EU law acquis there is no clearly defined concept of 'vulnerabilities.' The category covers most prominently children/minors and disabled people, those who are protected by EU non-discrimination law and, last but not least, vulnerable groups as specified in the UCPD, Art. 5 (3). There are some loose ends – economic vulnerabilities and digital literacy – but there is no overarching approach, neither in the EU consumer law acquis – substantive law and procedural law (ADR/ODR) – nor in the upcoming EU digital law acquis to guide what kind of measures the EU, the European Commission or the Member States should employ to adequately protect those claimed to be vulnerable.

Particularly striking is, if any, the focus on substantive law, whereas the well-known vulnerabilities in dispute resolution are just left out. One might argue that it is not for the EU to tackle the issue as it does not have genuine competence for law enforcement. In light of the competence creep and the willingness of the majority of Member States to accept an ever-stronger Europeanisation of law enforcement, this argument does not sound convincing. The omission is even more striking as the barriers in law enforcement, particularly for the 'vulnerable groups' in society, are well-researched and well-known to everybody who studies the access to justice movement and in well-documented empirical research.

76 On the burden of proof, but also far beyond in reply to the fairness deficit of the EU digital policy legislation, see Micklitz, HW, Helberger N., Namyslowska N., Naudts L., Rott P., Sax M. and Veale M. (2024), Towards Digital Fairness, EuCML, 24.

77 Duivenvoorde, B.B. (2023), Redesigning the UCPD for the Age of Personalised Marketing. EuCML 177.

Academic research[78] has gone beyond the current acquis and developed a more comprehensive understanding of 'vulnerabilities.' Provided one takes the concept of the structural, architectural and universal character of digital vulnerabilities seriously, the following challenges emerge:

Any online dispute resolution mechanism should have an architecture implementing diversity by design, a structure that the average customer can understand.

If it is successfully established and used in practice, the architecture might build a long-term relationship between the provider and the customer, thus strengthening their dependence in the same way that other platforms are doing (or other services, as we are not developing a platform). Whether the potential choice between different providers in different Member States may avoid building long-term relations will depend on whether there is competition and whether the customer can handle the competition. If the assumption is correct that there will be a blossoming market of providers offering different services under different conditions, customers might find themselves in a situation similar to the messy field of labels, in which they may easily get lost.

Development of the architecture, so far, is in the hands of computer scientists, software developers and, in the most comprehensive case, lawyers. Precautionary measures are needed to involve potential customers and civil society organisations.

78 See the Deliverable 5.1 - e-Justice ODR scheme, drafted in the framework of the DG Justice-supported project 'e-Justice ODR scheme' (GA n. 101046468), available at https://cjc.eui.eu/projects/odr-scheme/.

PART III
Contexts and Images of Digital Vulnerable Subjects

The Digital Vulnerability of Insurance Consumers and Personalised Pricing of Insurance Products*

Piotr Tereszkiewicz, Katarzyna Południak-Gierz, Patryk Walczak

A. Introduction

Modern technologies enable traders to personalise (individualise) contracts they conclude with consumers. Big data analytics has made it technically possible and commercially attractive to create profiles for individual consumers and provide them with personalised offers. The personalisation of content presented to online users has thus become a highly relevant legal issue. One is tempted to start by defining the notion of 'personalisation' itself.[1] Usually, personalisation is understood to mean the process of adjusting the online content presented to individuals depending on the data available on their situation, traits, and preferences.[2] The definition of personalisation may yet depend on whose perspective is assumed to describe it. From the perspective of the consumer, different methods of matching the content with the user may qualify as personalisation. These methods may all lead the consumer to believe that online content was tailored individually for them. If we understand personalisation in this manner, then it only occasionally entails *actual individualisation*: the content may be adjusted not to an individual user, but to the context in which the information is presented (e.g., context advertising) or to the typical characteristics of a targeted group (segment) of the population. Understood in this manner, personalisation is an umbrella term encompassing practices during which not only an individual but also a group of individuals can be the addressee (target), in particular, practices such as online contextual, segmented, and

* This Chapter has been written within the framework of a research project supported by the National Science Centre (NCN) in Poland, grant number 2018/29/B/HS5/01281.

1 We rely here on an excerpt from: Katarzyna Południak-Gierz and Piotr Tereszkiewicz, 'Digitalization's Big Promise and Peril: Personalization of Insurance Contracts and its Legal Consequences' in Klaus Mathis and Avishalom Tor (eds.), Law and Economics of the Digital Transformation, (Springer 2023) 34.

2 Eliza Mik, 'The erosion of autonomy in online consumer transactions' (2016) Law, Innovation and Technology 8, 19.

behavioural advertising.[3] Nevertheless, to define personalisation one can also assume a perspective which places technology at the centre. From this perspective, personalisation can be understood as a practice that involves using data collected from an individual's activity (e.g., purchase history, email activity, website behaviour) in order to deliver targeted content to that individual. Under this second approach, the terms 'individualisation' and 'personalisation' can be used interchangeably to describe the process in which the content is individually shaped for every addressee separately, based on their profile.[4]

Personalisation of contracts may, *inter alia*,[5] include personalisation of prices offered to individual consumers: typically, 'personalised pricing' oc-

3 Niklas Fourberg, Serpil Taş, Lukas Wiewiorra, Ilsa Godlovitch, Alexander De Streel, Herve Jacquemin, Jordan Hil, Madalina Nunu, Camille Bourguigon, Florian Jacques, Michele Ledger and Michael Lognoul, *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice*, Publication for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2021, 30-31; Christopher Townley, Eric Morrison and Karen Yeung, 'Big data and personalised price discrimination in EU competition law' (2017) 36 Yearb Eur Law, 689-690.

4 See Florent Thouvenin, Fabienne Suter, Damiane George and Rolf H. Weber, Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts' (2019) 10 JIPITEC, 210; Joanna Strycharz, Guda van Noort, Natali Helberger and Edith Smit, 'Contrasting perspectives – practitioner's viewpoint on personalised marketing communication' (2019) 54 European Journal of Marketing, 641; Marta Infantino, 'Big data analytics, insurtech and consumer contracts: a European appraisal' (2022) 30 Eur Rev Priv Law, 613; Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax and Joanna Strycharz, *EU consumer protection 2.0, structural asymmetries in digital consumer markets* (2021) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf>, 102; Południak-Gierz and Tereszkiewicz (n 1), 34. Personalisation mechanisms frequently rely on predictive analytics using big data sets – information fuelling the personalisation process is not only derived from the data on this person but also from other data sets on 'similar consumers' and statistical data, Mik (n 2), 20. The better the latter proxies are, the less information is needed about the actual preferences of an individual. Consequently, it can be argued that during the process of tailoring the information the point of reference is not a particular individual. The benchmark is the 'alter ego' of that individual, their digital representation construed within the digital environment, mostly for commercial purposes. This creates a problem which can be referred to as de-personalisation by personalisation tools, see Helberger, Lynskey, Micklitz, Rott, Sax and Strycharz (n 4), 103-104; Infantino (n 4).

5 In insurance (as well as in other instances where a specific risk is one of the crucial factors determining the values exchanged under a contract) personalisation of contracts may also take place solely with respect to provisions specifying insured

curs when traders use the data that they have collected to infer consumers' willingness to pay.[6] Even though the empirical evidence might be inconclusive, economic research suggests that personalised pricing, including price discrimination, does occur in practice.[7] In an extreme scenario, firms can set individual prices and fully extract consumers' willingness to pay to their economic advantage. In practice, traders usually employ indirect methods of personalised pricing, such as personalised discounts[8] or search discrimination.[9] Yet, as consumers end up paying different, personalised

risks, without extending to the personalisation of price because 'an insurance provider might have an interest in providing coverage (and therefore to engage in terms personalization) for additional events without raising the premium, as long as it does not increase its actual risk. (…) term personalization can play a major role in selecting how to include superabundant coverage and, at the same time, exclude relevant risks,' Antonio Davola, Fabrizio Esposito and Mateusz Grochowski, 'Price Personalization vs. Contract Terms Personalization' in Fabrizio Esposito and Mateusz Grochowski (eds), Cambridge Handbook on Price Personalization and the Law (Cambridge University Press, forthcoming).

6 Marc Bourreau and Alexandre de Streel, *The regulation of personalised pricing in the digital era* (OECD 2020) <https://one.oecd.org/document/DAF/COMP/WD(2018)150/en/pdf>, 2: 'We refer to both individual pricing and group pricing with small targeted groups as personalised pricing or price targeting'. Maurits Kaptein and Petri Parvinen 'Advancing E-Commerce Personalization: Process Framework and Case Study' (2015) 19 International Journal of Electronic Commerce, 9; Joost Poort and Frederik Zuiderveen Borgesius, 'Does everyone have a price? Understanding people's attitude towards online and offline price discrimination' (2019) 8 Internet Policy Review, 1.

7 Bourreau and de Streel (n 6), 3; Cristina Poncibò, 'The UCTD 30 Years Later: Identifying and Blacklisting Unfair Terms in Digital Markets' (2023) 19 European Review of Contract Law, 336.

8 Personalised discounts are very difficult to compare, which reduces the probability of consumers' negative reactions. Lan Xia, Kent B. Monroe and Jennifer L. Cox, 'The price is unfair! A conceptual framework of price fairness perceptions' (2004) 68 Journal of Marketing, claim that consumers may perceive personalised pricing as unfair, in particular when they observe they are paying a higher price for a similar product than other consumers. See also Kelly Haws and William Bearden, 'Dynamic Pricing and Consumer Fairness Perceptions' (2006) 33 Journal of Consumer Research, 304: price discrimination will often be regarded as unfair if it exceeds a certain level; Simon Lee, Abdou Illia and Assion Lawson-Body, 'Perceived price fairness of dynamic pricing' (2011) 111 Industrial Management & Data Systems, 531. For a different view Edwards (2006), 559.

9 Search discrimination or steering consists of showing different products to consumers from different groups, based on the available information about consumers, Bourreau and de Streel (n 6), 3.

net prices in such cases, those pricing strategies are equivalent to personalised pricing.[10]

Insurance is certainly one of business sectors in which the use of big data analytics has influenced the marketing and distribution stage in the value chain, enabling the rise of personalised insurance policies.[11] From a legal perspective, these developments merit close attention as technology based marketing and distribution strategies fall within the scope of EU consumer protection and data protection frameworks to which this Chapter will turn below.

B. Digital distribution of insurance and personalisation of insurance contracts

In the insurance sector, there are two most important criteria for the personalisation (individualisation) of insurance contracts.[12] First, personalisation is typically based on the risk profile of the consumer. In practice, insurers do not calculate the risk for each consumer but create groups of customers and offer premiums corresponding to the risk assessment for respective groups.[13] Insurance premiums reflect the assessments concerning the risk to be insured against.[14] Second, personalisation may be undertaken based on the consumer's willingness to pay (price optimisation).[15] Insurance regulators describe price optimisation as an insurer's use of sophisticated data mining tools and modelling techniques during the ratemaking

10 Bourreau and de Streel (n 6), 3.

11 Antonella Cappiello, *Technology and the Insurance Industry. Re-configuring the Competitive Landscape* (Palgrave Macmillan 2018); Bernardo Nicoletti, *Insurance 4.0. Benefits and Challenges of Digital Transformation* (Palgrave Macmillan 2021).

12 In this Chapter, 'personalisation' and 'individualisation' will be treated as synonyms. Thouvenin, Suter, George and Weber (n 4), 210, use the term 'individualisation' of insurance contracts with respect both to the consumer's willingness to pay and the consumer's risk profile.

13 Thouvenin, Suter, George and Weber (n 4), 211, indicating that this serves two important policy goals: the reduction of adverse selection and the avoidance of moral hazard.

14 Casualty Actuarial Society, *Generalised Linear Models for Insurance Ratings* (2nd edn, CAS Monograph Series No. 5 2020), available at https://www.casact.org/sites/default/files/2021-01/05-Goldburd-Khare-Tevet.pdf.

15 Thouvenin, Suter, George and Weber (n 4), 242; Barış Soyer, 'Use of Big Data Analytics and Sensor Technology in Consumer Insurance Context: Legal and Practical Challenges' (2022) 81 Cambridge Law Journal.

process to vary rates based on factors other than a person's risk of loss.[16] This means that insurers use non-causal risk proxies (e.g., shopping habits or internet searches) to determine whether a potential consumer is willing to pay more for the same product as opposed to others who are in the same risk profile.[17] Personalisation based on the consumer's willingness to pay results from the fact that consumers with a uniform or similar risk profile may have different needs for insurance cover, and perhaps more importantly, different financial resources for buying insurance products.

Undoubtedly, these two main criteria for personalising insurance contracts may be combined in practice when calculating the individual premium of a customer.[18] One must bear in mind that technological solutions used in the insurance industry automatically collect personal data about consumers, thus automatically performing a risk analysis according to a pre-defined algorithm, which in the end entails determining the price for the risk assumption by the insurer.[19] During this process, different types of data relevant for targeting a consumer are gathered and analysed.[20] What is crucial is that these data may be used not only for narrow actuarial purposes, i.e., calculating a premium, but also to increase the profit that an insurance distributor derives from a transaction. For instance, marketing techniques can be oriented towards artificially increasing consumers' willingness to pay, so that they opt for more expensive insurance products[21] or differentiating the price for different policyholders interested in purchasing the same insurance product.[22]

16 The Research Report, 'The Use of Price Optimization in Insurance Ratemaking', the Connecticut General Assembly <https://www.cga.ct.gov/2015/rpt/2015-R-0251.htm>.

17 Soyer (n 15), 183.

18 Thouvenin, Suter, George and Weber (n 4), 242.

19 Mário Čertický, 'Certain Issues of Innovations Affecting the Insurance Business in the in the Light of the GDPR and Hungarian Insurance Law' (2021) 10 Acta Universitatis Sapientiae Legal Studies, 51.

20 As to categories of personal data used for personalisation (individualisation) see Thouvenin, Suter, George and Weber (n 4), 210-211; Čertický (n 19), 38; Helberger, Lynskey, Micklitz, Rott, Sax and Strycharz (n 4), 103–104; Soyer (n 15), 169-170.

21 Peter Rott, Joanna Strycharz and Frank Alleweldt, *Personalised Pricing* (Publication for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, 2022), 8; Oren Bar-Gill, 'Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis)perceptions' (2019) 86 University of Chicago Law Review, 218.

22 Piotr Tereszkiewicz and Katarzyna Południak-Gierz 'Liability for Incorrect Client Personalization in the Distribution of Consumer Insurance' (2021) 9 Risks, 84; for

There is no general principle of insurance law that forbids personalising (individualising) insurance prices (premiums).[23] It is worthwhile to emphasise that in the European Union, the requirement of prior approval of standard terms was abolished as a result of the deregulation of the insurance sector in 1992.[24] As a result of this revolutionary development, the internal market directives, both in life and non-life insurance, have introduced the formal prohibition of prior approval or systematic notification of general and special policy conditions, scales of premiums, or forms and documents which an insurance undertaking intends to use.[25] Article 181(1) of the Solvency II Directive provides that Member States shall not require the prior approval or systematic notification of general and special policy conditions, scales of premiums, or forms and other printed documents which an insurance undertaking intends to use in its dealings with policyholders. Under Article 181(2) Solvency II, Member States which make insurance compulsory may require that insurance undertakings communicate to their supervisory authority the general and special conditions of such insurance before circulating them.

By contrast, there might be specific provisions in different fields of law, possibly relating to different branches of insurance.[26] In this respect, U.S. law provides an interesting example. In the U.S. the insurance business is primarily regulated at a state level.[27] Most state insurance laws in the U.S. provide that 'insurance must be fair, available, and affordable'. Insurance rates are subject to statutory requirements: insurance rates cannot be excessive, inadequate, or unfairly discriminatory. Further, in most states

examples of such practices using data exploration see Zarsky, '"Mine Your Own Business!": Making The Case For The Implications Of The Data Mining Of Personal Information In The Forum Of Public Opinion' (2003) 5 Yale Journal of Law and Technology, 19-21.

23 For an in-depth survey of Swiss and California legal systems Thouvenin, Suter, George and Weber (n 4), 242; see also Soyer (n 15).

24 Herman Cousy, 'Insurance law between business law and consumer law. Belgian report' in Eric Dirix and Yves-Henri Leleu (eds), *The Belgian Reports at the Congress of Washington of the International Academy of Comparative Law* (Brulyant 2011), 549.

25 Idem.

26 Thouvenin, Suter, George and Weber (n 4) provide a comparative overview of the laws applicable to the individualisation of insurance contracts in Switzerland and California/US.

27 See Tom Baker, Kyle D. Logue and Carolyn V. Williams, *Insurance Law and Policy: Cases and Materials* (Wolters Kluwer 2021), 613. Federal regulation does not play a significant role in governing the insurance business except for some federal statutes on health insurance.

property and casualty insurance rates have to be approved by state commissioners prior to use by insurers. Statutory protection against arbitrary insurance rates can be extended to prohibit personalised pricing as has become the case in the California insurance regulation: personalisation (individualisation) based on the consumer's willingness to pay in property and casualty insurance is straightforwardly excluded by way of a notice issued by the Insurance Commissioner in February 2015.[28] The Commissioner's Notice defines price optimisation as 'any method of taking into account an individual's or class's willingness to pay a higher premium relative to other individuals or classes'. The Notice states that price optimisation does not seek to arrive at an actuarially sound estimate of the risk of loss and other future costs of a risk transfer. In the Commissioner's view, any use of price optimisation in the ratemaking or pricing process is unfairly discriminatory and violates California law. It follows that under California insurance law there is no leeway for the personalisation of insurance contracts based on the consumer's willingness to pay. Importantly, several other state jurisdictions in the U.S. have followed California in barring the use of price optimisation in the ratemaking process.[29]

In what follows, we analyse market practices that involve the personalisation of insurance contracts in the light of GDPR and UCPD.[30] The question of the personalisation of insurance contracts appears particularly relevant as far as the interplay between those two regulatory regimes is concerned. Since data collection processes are essential in the insurance business and the use of personalisation tools is increasing in this sector,[31] there is always a possibility that personalisation tools might be applied in violation of GDPR to maximise the traders' profits. Should this happen, a trader's conduct

28 <https://www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/PriceOptimization.pdf>. See Thouvenin, Suter, George and Weber (n 4), 218.

29 For a brief description see the Research Report 'The Use of Price Optimization in Insurance Ratemaking', the Connecticut General Assembly <https://www.cga.ct.gov/2015/rpt/2015-R-0251.htm>.

30 The analysis of the personalisation of insurance contracts under anti-discrimination law remains outside the scope of this Chapter; see Thouvenin, Suter, George and Weber (n 4), 220-227.

31 Thouvenin, Suter, George and Weber (n 4), 227; Piotr Tereszkiewicz, 'Digitalisation of Insurance Contract Law: Preliminary Thoughts with Special Regard to Insurer's Duty to Advise' in Pierpaolo Marano and Kyriaki Noussia (eds) *InsurTech: A Legal and Regulatory View. AIDA Europe Research Series on Insurance Law and Regulation*, vol 1. (Springer 2021), 127; Soyer (n 15), 166-167.

would certainly fall within the scope of UCPD as a potentially unfair commercial practice.

It must be stressed that the data analysed and processed for the individualisation (personalisation) of insurance contracts are typically the consumer's personal data hence they raise questions concerning privacy and data protection law; in the light of Article 4(1) GDPR, all the information relating to the data subject is personal data.[32] As far as sensitive data is concerned, the processing of genetic, biometric and health data of the data subject may typically arise in the context of insurance relationships.[33]

C. Personal data processing under GDPR

Under the General Data Protection Regulation (subsequently referred to as GDPR)[34] every processing of personal data[35] must have a lawful basis, such as consent of the data subject or a legitimate interest of the controller. Moreover, the processing must be carried out in accordance with the applicable data protection principles, which GPRD lays down as follows.

First, the data minimisation principle requires that the collection of personal data should be limited to what is necessary for the purposes for which they are processed (Article 5(1)(c)). Second, under the GDPR's accuracy principle, personal data must be accurate and kept up to date (Article 5(1)d). Data controllers are responsible for ensuring the accuracy of the data they compile about consumers, even if the data has been obtained from other sources. Third, the storage limitation principle of GDPR obligates data controllers to limit the storage of personal data to the timeframe necessary for their processing (Article 5(1)(e)). Fourth, the integrity and confidentiality principle requires data controllers to implement appropriate technical and organisational measures to ensure the security of personal data (Article 5(1)(f)). Finally, Article 20 of GDPR grants consumers a right to data portability, which allows them as data subjects to obtain from

32 Thouvenin, Suter, George and Weber (n 4), 227; Bourreau and de Streel (n 6), 6; Čertický (n 19), 38.

33 Čertický (n 19), 40, points out that such processing may arise in connection with fixed-sum insurance, specifically life and accident insurance as well as liability insurance.

34 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1.

35 Under Article 4(1) GDPR any information relating to an identified or identifiable natural person ('data subject') is considered personal data.

data controllers the personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

Typical examples of GDPR breaches by a trader may include: i) processing personal data without a proper legal basis; ii) processing special categories of personal data based solely on Article 9 GDPR, and without the explicit consent of the data subject; iii) using automated decision-making without any legal basis; and iv) failing to comply with information duties imposed by the GDPR. While these conduct types are discussed in the legal literature,[36] an assessment of whether the personalisation of insurance premiums is carried out in compliance with the GDPR may still pose a significant challenge in practice. Three major difficulties arise. First, one should note that the legal basis for processing personal data by an insurance distributor may differ depending on, among other factors, the relevance of data for a risk assessment by an insurance distributor.[37] Second, data processing within the insurance sector is highly automated, and therefore it needs to be verified as to whether automated data processing – a stage preliminary to decision-making – falls within the scope of Article 22(1) GDPR, and if so, whether it is covered by the exception provided for in Article 22(2) GDPR (see below). Third, verifying whether the process that leads to the personalisation of insurance premiums is sufficiently transparent may also be problematic.

I. Lawfulness of data processing under GDPR

From the perspective of the insurance business, personal data of consumers is necessary for both a risk assessment and the offering of adequate insurance products by insurance distributors.[38] Under the GDPR, the legal

36 Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

37 Viktoria Chatzara, 'The Interplay Between the GDPR and the IDD' in Pierpaolo Marano and Kyriaki Noussia (eds) Insurance Distribution Directive (Springer 2021), 281.

38 On using processing data to prepare an offer see Ulrich Damman and Spiros Simitis, *EG-Datenschutzrichtlinie: Kommentar* (Nomos 1997), 149; Chatzara (n 38), 281.

basis for processing that personal data may be the 'processing necessity':[39] under Article 6(1)(b) GDPR, 'Processing shall be lawful if (…) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract.' 'Necessity' means that the purpose of the processing could not be fulfilled with anonymous information.[40]

The concept of 'processing necessity' is based on the conclusive consent of the data subject, i.e., the consumer.[41] The necessity of personal data processing requires investigating whether there are less intrusive means of assuring the appropriate performance of a contract, especially if the contract could be performed without the processing of personal data.[42] If that is the case, the necessity criterion under the GDPR is not fulfilled.[43] Further, Article 6(1)(b) GDPR stipulates that data processing may be lawful if it is necessary 'in order to take steps at the request of the data subject prior to entering into a contract'. This could be the processing of personal data in order to prepare an offer.[44] Following the same rationale, data processing is usually necessary to supply an offer of an insurance product to the consumer. Thus, it can be argued that the provision of Article 6(1)(b) GDPR can be considered the most suitable ground for processing personal data that are relevant for risk assessment as the latter is crucial for preparing an offer. It follows that, in so far as the personal data that is processed serves to determine the risks that are to be insured and affects the risk pricing, the processing of such data might be viewed as lawful under Article 6(1)(b) *in fine* GDPR.[45] Consequently, insurance distributors

39 Waltraut Kotschy, 'Commentary to Article 6' in Kuner, Bygrave, Docksey and Drechsler (n 36), 331; Čertický (n 20), 45-46.

40 Judgment of the Court (Grand Chamber) of 16 December 2008, Heinz Huber v Bundesrepublik Deutschland, Case C-524/06, ECLI:EU:C:2008:724, para. 62 ff.

41 Kotschy (n 39), 331.

42 Kotschy (n 39), 331; Thouvenin, Suter, George and Weber (n 4), 232. In its 2/2019 Guidelines, the European Data Protection Board stated that only objectively necessary processing operations may be based on this legal ground; the contract cannot 'artificially expand' the categories of personal data or processing operations beyond the data subject's reasonable expectations, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (EDPB 2019), 8.

43 EDPB (n 42), 7.

44 Kotschy (n 39), 331.

45 It is submitted that the arguments raised in the analysis of whether this ground for processing can be invoked concerning price discrimination are not applicable in this context, see Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price

must carefully determine the personal data they need, to proceed with an accurate risk analysis, and collect from the consumer the data that is appropriate, adequate and necessary for such purposes in line with the data minimisation principle.[46] With respect to price personalisation based on the consumer's willingness to pay, it is submitted that the criterion of 'necessity' under GDPR may not be fulfilled. For the insurer can always rely on risk groups and is not obligated to personalise insurance contracts.[47] It follows that insurance distributors should rely on other grounds for the lawfulness of processing in cases involving the personalisation of insurance contracts, i.e., the consent of the consumer.

Further, one should emphasise that insurance distributors are obliged to explore the needs and wishes of clients and provide adequate explanations and advice.[48] These obligations result from the Insurance Distribution Directive[49] and national provisions on insurance contract law.[50] With respect to personal data that must be processed to comply with the above-mentioned obligations – i.e., data required to establish what insurance cover a consumer needs or wishes to obtain, the legal basis for processing shall be found in Article 6(1)(c) GDPR. Although Article 6(1)(c) GDPR does not usually justify data processing for marketing purposes in e-commerce,[51] it might provide a legal basis for data processing by insurance distributors: Specifically where the data is used to match the scope of products to be offered to consumers to meet their needs.[52] However, Article 6(1)(c) GDPR does not allow an insurance distributor to process that data for the purposes of the personalisation of the insurance premium as neither of

Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy, 360.

46 Chatzara (n 37), 282; Thouvenin, Suter, George and Weber (n 4), 230.

47 Thouvenin, Suter, George and Weber (n 4), 232.

48 Piotr Tereszkiewicz, *Obowiązki informacyjne w umowach o usługi finansowe* (Wolters Kluwer Polska 2015), 297-299; Tereszkiewicz (n 32), 142; Chatzara (n 38), 282.

49 Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution [2016] OJ L 26/19.

50 See Południak-Gierz and Tereszkiewicz (n 1), 42-44.

51 Katarzyna Południak-Gierz, Consequences of the use of personalization algorithms in shaping an offer – a private law perspective' (2019) 13 Masaryk University Journal of Law and Technology 2, 176.

52 Guidelines 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 (2021), Official 2021/C 526/01, 18; On when such an obligation arises in the context of e-commerce see Tereszkiewicz and Południak-Gierz (n 22).

the abovementioned insurance distributor's obligations requires them to personalise insurance contracts based on the consumer's willingness to pay.

Finally, some personal data are processed by insurance distributors not because they are essential for risk assessment at the pre-contractual stage or because of the need to comply with the legal obligations of insurance distributors, but just for marketing purposes. In such cases, it could either be argued that processing is necessary for the purposes of the legitimate interests pursued by the controller (Article 6(1)(f) GDPR) or that the lawfulness of such personal data processing will depend on whether the data subject has consented to the processing of their personal data for these specific purposes (Article 6(1)(a) GDPR).

Further, under Article 6(1)(f) GDPR data processing is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data. It could be argued that an insurance distributor has a legitimate interest in processing personal data for the assessment of insurance risk and the calculation of insurance rates. As long as the data taken into account is relevant from the perspective of risk assessment, it is reasonable to assume that, in principle, the controller has a legitimate interest in their processing and that interest is not overridden by the interests or fundamental rights and freedoms of the data subject. This might change once other data is analysed during the process of underwriting, especially if non-risk-relevant personal data is referred to and consequently, the premium calculated based on risk-relevant factors increases to match the insurance consumer's willingness to pay. Here, even if one were to conclude that there are no better-suited and less intrusive ways of safeguarding insurance distributor's interests (which is, however, unlikely), one might be inclined towards a view that the interests of the consumer and especially the right to privacy should override the aforementioned economic interests of the insurance distributor.[53] At the very least,

53 Agnieszka Jabłonowska, Francesca Lagioia and Giovanni Sartor in Fabrizio Esposito and Mateusz Grochowski (eds), Cambridge Handbook on Price Personalization and the Law (Cambridge University Press, forthcoming) argue that generally in the case of price personalisation, the consumer's interests outweigh those of the controller except for instances where personalisation cannot negatively affect the consumers' economic interest, e.g., consists solely in offering individualised discounts. Similarly Fabrizio Esposito, 'The GDPR Enshrines the Right to the Impersonal Price' (2022) 45 Computer Law & Security Review, 7, 12.

an approach based on the balancing of conflicting interests requires a case-specific assessment; a universal interest analysis is impossible.[54]

As for the consumer's consent to having their personal data processed, consent should be freely given, without any pressure;[55] otherwise, it will not be valid.[56] Further, the data subject ought to be informed about the specific purpose of data processing in a way that enables that data subject to understand the intended result of data processing. The main difficulty in this regard lies in the assessment of whether the aforementioned purpose was communicated in a sufficiently clear and precise manner. The technical jargon of insurance law makes it difficult for consumers to understand why their personal data is processed.

What is more, one should emphasise that one and the same piece of data could be used for more than one purpose. If these purposes are not compatible with one another, then an appropriate legal basis for the processing is required for each of these purposes.[57]

Finally, one should take into account the scope of data processed by an insurance distributor as it may cover data that fall within special categories of personal data provided for in Article 9(1) GDPR.[58] Consequently, the lawfulness of processing that data depends on whether, in addition to being covered by one of the situations listed in Article 9(2) GDPR, the requirements of Article 6 GDPR are met in a given case.[59] With respect

54 Thouvenin, Suter, George and Weber (n 4), 234.

55 Kotschy (n 39), 330.

56 Article 29 Data Protection Working Party Opinion (2011) 15/2011 on the definition of consent, 13.

57 Cécile de Terwange, 'Commentary to Article 5' in Kuner, Bygrave, Docksey and Drechsler (n 36), 315-316; Article 29 Data Protection Working Party 'Opinion (2013) 03/2013 on Purpose Limitation, 40; Thouvenin, Suter, George and Weber (n 4), 232. Soyer (n 15), 176, emphasises practical difficulties for insurers in complying with that requirement and recommends imposing specific restrictions on insurance companies' capacity to repurpose data. See also Paul MacDonnell, 'The European Union's Proposed Equality and Data Protection Rules: An Existential Problem for Insurers' (2015) 35 Economic Affairs, 233, observing that insurers using data mining techniques do not know what they will find until it is too late.

58 Jeffrey Amankwah and Nele Stroobants, 'GDPR and the Processing of Health Data in Insurance Contracts: Opening a Can of Worms?' in Margarida Lima Rego and Birgit Kuschke (eds) *Insurance and Human Rights. AIDA Europe Research Series on Insurance Law and Regulation,* vol *5.* (Springer 2022), 179.

59 Ludmila Georgieva and Christopher Kuner, 'Commentary to Article 9' in Kuner, Bygrave, Docksey and Drechsler (n 36), 376.

to this category of personal data,[60] one should point out that if such data is disclosed at the pre-contractual stage, explicit consent for its processing should be obtained. This requires a high standard of determining the purpose of processing and a precise wording of the respective consent[61] under Article 9(2)(a) GDPR) even if the requirement of processing necessity is fulfilled, as may be the case under Article 6(1)(b) GDPR and there is room for an implied consent. So as long as sensitive data is processed by an insurance distributor, explicit consent from the data subject is required; implied consent is not sufficient.

II. GDPR and automated individual decision-making

When it comes to fully automated individual decision-making that produces legal effects concerning the data subject or similarly significantly affects that data subject,[62] explicit consent to the processing of personal data is required under Article 22(2)(c) GDPR.[63] Personalising insurance prices could be an example of automated individual decision-making: Within this process, the algorithm decides on the price for a specific consumer, in a fully automated manner, and this affects the legal situation of the consumer as the process determines the extent of their contractual obligations should a contract be concluded.[64] Similarly, data processing based on Internet of Things (IoT) systems is regarded as automated decision-making, including profiling.[65] This suggests that where insurance distributors want to use automated processing for this purpose, even though the data processing it-

60 With the exception of employment and social security law.

61 Georgieva and Kuner (n 59), 377; Amankwah and Stroobants (n 58), 195; Soyer (n 15), 174.

62 On the nature of profiling and automated decision-making see Aleksandra Drożdż, *Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR* (Wolters Kluwer 2019), 10–16.

63 Lee A Bygrave, 'Commentary to Article 22 GDPR' in Kuner, Bygrave, Docksey and Drechsler (n 36), 537; Drożdż (n 62), 54–57.

64 Isak Mendoza and Lee Bygrave, 'The Right Not to be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou Synodinou, (eds) *EU Internet Law* (Springer 2017), 93. The CJUE has adopted a broad interpretation of 'automated individual decision-making' in the judgment of 7 December, Case C-634/21, OQ v Land Hessen, ECLI:EU:C:2023:957, para. 73.

65 Čertický (n 19), 45.

self is lawful under Article 6 GDPR alone or Article 6 GDPR in conjunction with Article 9 GDPR, they have to obtain additional consent from the data subject for the automation of data processing.[66]

However, the above requirement does not apply if automated individual decision-making is necessary for entering or performing a contract between the data subject and a data controller, or is authorised under EU or national law to which the controller is subject,[67] and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.[68] In the light of the above, in some instances, automation of the underwriting process might be allowed based on national law, while in others it is necessary to examine if automated individual decision-making was necessary for entering or performing a contract between the data subject

66 This applies to real-time, continuous data recording concerning the insured consumer as a data subject, Čertický (n 19), 48. See also EDPB (2020) *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*.

67 See, under Polish law, Article 41 of the Act on Insurance and Reinsurance Business of 11 September 2015 (Law Journal of 2023, item 656) which states that:
Section 1a. The insurance company may make decisions in individual cases based solely on automated processing, including profiling, of personal data in order to:
1) assess the insurance risk – in the case of personal data relating to the insured persons,
2) performance of insurance activities referred to in Article 4 Section 9 points 1 and 2 – in the case of personal data relating to the insured, policyholders and persons entitled under the insurance contract
– provided that the person affected by the automated decision is given a right to receive appropriate explanations as to the basis for the decision, to protest the decision, to express his or her position and to obtain human intervention.
Section 1b. The decisions referred to in section 1a, may be made only on the basis of the following categories of data relating to a natural person: 1) name(s) and surname; 2) family name; 3) parents' names; 4) date and place of birth; 5) age; 6) gender; 7) citizenship; 8) PESEL number, if assigned; 9) tax identification number, if assigned; 10) number and series of ID card or other document confirming identity; 11) nature of work performed (sector); 12) place of residence; 13) insurance period; 14) insurance history; 15) sum insured; 16) marital status; 17) health condition of the insured person; 18) financial situation; 19) date and number of damage registration, date of damage occurrence, and date of reporting the damage or claim; 20) identifying the insurance contract to which the damage relates; 21) identifying the subject of insurance; 22) the number, type and dates of offenses or crimes constituting violations of road traffic regulations, including driving under the influence of alcohol or under the influence of alcohol or substances acting similarly to alcohol; 23) the number of points assigned to violations of road traffic regulations referred to in point 22, and the amount of fines imposed by way of a penalty notice and the fact of their payment.

68 Bygrave (n 63), 536-538; Čertický (n 19), 48-49.

(the consumer) and the data controller (the insurance distributor).[69] One should remark with caution that there appears to be no clarification as to how this criterion of 'necessity' should apply in practice, so it is ultimately left to courts to determine.[70] Nonetheless, the criterion of 'necessity' cannot be fulfilled where the personalisation of insurance contracts is not mandated by law but merely results from the commercial practices of insurance distributors.

III. Information duties on data processing under GDPR

Since the approach of EU law towards data processing is based on the consent-notice model, the information duties of data controllers form an important part of the GDPR.[71] Consequently, an insurance distributor as a data controller is required to inform the data subject about the processing of their personal data regardless of whether personal data is obtained from the data subject (Article 13 GDPR) or an external source (Article 14 GDPR). Information duties imposed under Article 13 GDPR must be fulfilled when personal data is collected, not after that, and also every time personal data is gathered.[72] When personal data is collected from an external source, then information duties are to be fulfilled in a reasonable time, no later than one month after the data has been collected.[73]

Information that must be provided includes the identity and contact details of the controller and, where applicable, of the controller's representative, the contact details of the data protection officer. Furthermore, the purposes of the processing for which personal data is intended need to be indicated as well as the legal basis for the processing and other matters set out in Article 13(1), Article 13(2), Article 14(1), and Articles 14(2) GDPR. Information about the purposes of processing is particularly important as exceeding the scope of the specified processing purposes, and herewith

69 Cf. in detail Čertický (n 19), 41-42.
70 Soyer (n 15), 175, observes that it is unlikely that the criterion of being 'necessary' connotes indispensability.
71 Thouvenin, Suter, George and Weber (n 4), 227.
72 Gabriela Zanfir-Fortuna, 'Commentary to Article 13 GDPR' in Kuner, Bygrave, Docksey and Drechsler (n 36), 425–427; Rossana Ducato, 'Data protection, scientific research, and the role of information' (2020) Computer Law and Security Review, 10.
73 Zanfir-Fortuna (n 72), 445; Ducato (n 72), 10.

diverging from the initial purpose of processing infringes on Article 5(b)(1) GDPR.[74]

With respect to personal data processing within the framework of automated decision-making mechanisms, data controllers are obliged under the provisions of Articles 13(2)(f), 14(2)(g), and (15)(1)(h) GDPR to inform data subjects not only about the use of automated decision-making in personal data processing but also about the logic (assumptions) behind this mechanism.[75] However, the nature of this information duty is debated; specifically, it is contentious whether this duty can only be fulfilled *ex-ante* or also *ex-post*.[76]

In practice insurance distributors usually process large sets of personal data of insurance consumers for different purposes; the legal bases for that processing tend to differ in the context of each of these purposes. This alone makes it difficult to fulfil information obligations as achieving sufficient transparency of information is a challenge.

D. Personalised pricing of insurance products under Unfair Commercial Practices Directive

Under EU law, business conduct involving price personalisation in relation to consumers is subject to the assessment under the Unfair Commercial Practices Directive. The main objective of the Unfair Commercial Practices Directive is to protect consumers from the consequences of unfair commercial practices which could 'directly harm consumers' economic interests and thereby indirectly harm the economic interests of legitimate competitors'.[77] Most importantly, UCPD protects consumer economic interests from unfair business-to-consumer commercial practices and addresses commercial practices directly related to influencing consumers' transactional decisions concerning products.[78] It follows that market practices of an insurance distributor that involve processing personal data under GDPR are subject

74 Zanfir-Fortuna (n 72), 430.
75 Mendoza and Bygrave (n 64), 93; Jonas Knetsch, 'Data Protection Rights and Automated Decision-Making in the Field of Insurance' in Cristina Poncibò and Piotr Tereszkiewicz (eds), *The Evolution of European Insurance Contract Law in the Digital Age* (Springer forthcoming), passim; Rott, Strycharz and Alleweldt (n 21), 27.
76 Mendoza and Bygrave (n 64), 93-94.
77 See recital 6 UCPD.
78 Idem.

to control under UCPD, if they harm the economic interest of consumers by influencing their transactional decisions. There are three consecutive tests for assessing whether a commercial practice may be considered unfair under UCPD.[79]

The first test is performed by analysing whether a relevant practice falls within the blacklist of unfair commercial practices annexed to UCPD. If this is the case, then such a practice is unconditionally regarded as unfair.[80] The second test requires an assessment of whether a relevant practice is misleading by action (Article 6 UCPD) or omission (Article 7 UCPD), or is aggressive (Article 8 UCPD).[81] Finally, there is an assessment of unfairness under the general clause of Article 5 UCPD: a commercial practice is unfair if 'it is contrary to the requirements of professional diligence' and it 'materially distorts or is likely to materially distort the economic behaviour about the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers'. To pass the fairness test of Article 5 UCPD, a commercial practice must satisfy both criteria laid down by this provision.

Under the above framework, establishing whether a trader's conduct involving personalising insurance prices contrary to GDPR qualifies as an unfair market practice requires the examination of the blacklist of unfair market practices as laid down in Annex I to Directive 2005/29/EC. Annex I contains commercial practices divided into two groups: misleading and aggressive.[82] Personalisation conducted in a manner inconsistent with GDPR

79 Jules Stuyck, Evelyn Terryn and Tom van Dyck, 'Confidence Through Fairness? The New Directive on Unfair Business-To-Consumer Commercial Practices in the Internal Market' (2006) 43 CMLRev, 132-134; Hans-Wolfgang Micklitz, 'The general clause on unfair practices' in Geraint Howells, Hans-Wolfgang Micklitz and Thomas Wilhelmsson (eds) *European Fair Trading Law The Unfair Commercial Practices Directive* (Routledge Taylor & Francis Group 2016), 85-86; Guidance on the interpretation and application of Directive 2005/29/EC (2021), 26.

80 Hans-Wolfgang Micklitz, 'Unfair commercial practices and misleading advertising' in Hans-Wolfgang Micklitz, Norbert Reich and Peter Rott, *Understanding EU Consumer Law* (Intersentia 2009), 88-89; Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking Eu Consumer Law* (Routledge Taylor & Francis Group 2018), 53.

81 Monika Namysłowska, 'Dziesięć lat dyrektywy 2005/29/WE o nieuczciwych praktykach handlowych' (2016) 3 Europejski Przegląd Sądowy, 5.

82 Micklitz (n 80), 111; Jules Stuyck, 'The Court of Justice and the Unfair Commercial Practices Directive' (2015) Common Market Law Review, 741; Howells, Twigg-Flesner and Wilhelmsson (n 80), 53.

is not included in the blacklist as such. Moreover, non-compliance with GDPR itself does not qualify as an example of blacklisted market practices. It appears that the first test of unfairness may be passed: personalising insurance prices without complying with GDPR does not qualify as one of the unfair commercial practices listed under Annex I.

However, it is important to observe that an amendment to Annex I has been recommended in the BEUC Report.[83] *Inter alia* adding the following practices was proposed:

> '(49) Practices including behavioural (algorithmic) pricing, as well as those involving personalised pressure, performed based on detailed profiles mapping a person's personality, biases and vulnerabilities (psychographic profiles) should always be deemed as unfair.
> (50) Similarly, digital commercial practices should be prohibited where they are using data which may reasonably be suspected to have been obtained in breach of data protection laws.'

This proposal merits attention given the dual character of its approach. Under Point (49) of the BEUC Report, prohibiting some of the sophisticated market practices based on and inextricably linked with personal data processing regardless of whether they are performed with the breach of GDPR has been recommended. The main justification relates to the concern that personalisation based on mapping one's personality, biases and vulnerabilities has an immense potential to distort consumer market behaviour in a manner that is unperceivable for the data subject when they consent to data processing. In contrast, under Point (50) of the BEUC Report, the sole fact that it may be reasonably suspected that data processed within the framework of a digital commercial practice has been obtained in breach of GDPR automatically leads to the qualification of such a commercial practice as unfair. It follows that a potential[84] breach of GDPR at the data-gathering stage 'poisons' all digital commercial practices that are undertaken using that data. Consequently, on this account practices involving any potential breach of GDPR would be considered to be unfair. A possible justification for such a robust approach would be that in the digital environment, it is very difficult to assess whether personal data were gathered in compliance with data protection laws, i.e., whether a data subject has been properly

83 *EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy* (BEUC 2022), 12.

84 It is sufficient that a breach can be reasonably supposed.

informed about the purpose of data processing. One could thus claim that for the prohibition to be effective in practice, the occurrence of a breach of GDPR does not have to be established, but only reasonably suspected.

The second test of unfairness under UCPD includes two steps.[85] First, it needs to be examined whether processing personal data in breach of GDPR can qualify as an aggressive practice, and second – if a breach of GDPR can be classified as a misleading practice. In both instances, one must establish whether the practice at hand causes or is likely to cause the consumer to make a transactional decision that he or she would not have taken otherwise.

Under Article 8 UCPD, a commercial practice shall be regarded as aggressive if, by harassment, coercion, including the use of physical force, or undue influence (Article 9 UCPD), it significantly impairs or is likely to significantly impair the consumer's ability to make a conscious decision,[86] in a manner that affects or is likely to affect his or her market behaviour, causing him to take a transactional decision that he would not have taken otherwise.

In principle, the personalisation of insurance prices itself cannot be classified as an aggressive commercial practice:[87] Adjusting the price of insurance products using processing personal data cannot be seen as significantly impairing – or being likely to significantly impair – consumers' freedom of choice by harassment, coercion, including the use of physical force, or undue influence. One can imagine a situation whereby an insurance distributor infringes on GDPR in order to cause a consumer to buy an insurance product. Specifically, using personal data, a trader can learn about sudden changes in the life of a consumer (e.g., the death of a family member, serious illness) and use this knowledge to exercise mental pressure to cause that consumer to buy an insurance product where the price is personalised. This would amount to exploiting '(...) specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision about the product' under Article 9(c) UCPD. Nonetheless, what makes such a

85 Howells, Twigg-Flesner and Wilhelmsson (n 80), 57-58.

86 Micklitz (n 80), 86; Mariusz Golecki and Piotr Tereszkiewicz, 'Taking the Prohibition of Unfair Commercial Practices Seriously' in Klaus Mathis, Avishalom Tor (eds), *New Developments in Competition Law and Economics. Economic Analysis of Law in European Legal Scholarship*, vol *7* (Springer 2019), 91.

87 Bourreau and de Streel (n 6), 6, claim it is currently unclear under which circumstances personalised prices can be considered an unfair commercial practice.

practice an aggressive commercial practice under UCPD is neither price personalisation nor a GDPR breach *per se*, but rather the fact that in such cases the requirements of Article 8 UCPD are met. There are undoubtedly cases where a commercial practice will, at the same time, infringe on GDPR and be considered aggressive under Article 8 UCPD; but this does not necessarily entail that it is a GDPR breach that makes such a practice an aggressive market practice.

Further, Articles 6 and 7 of UCPD introduce a specific prohibition of misleading commercial practices. Specifically, Article 6(1) UCPD prohibits commercial practices containing false information that are, therefore, untruthful or in any way, including overall presentation, deceive or are likely to deceive an average consumer, even if the information is factually correct. In principle, misleading information should concern the existence or nature of the product, its main characteristics, price, maintenance, the trader, or consumer rights.[88]

Article 6(1)(d) UCPD has a significant function for the assessment of whether price personalisation practices are allowed: it prohibits practices that mislead or are likely to mislead a consumer, even if they contain the factually correct information, on price or its calculation method – without limitation to the subject matter on which the price is determined. Thus, the use of personalised discounts or overpricing insurance products based on certain personal data may be considered misleading in cases where consumers are misinformed as to how insurance premiums and related costs were calculated.[89] Specifically, an insurance distributor may inform the consumer that the insurance price was tailored for them (or even specify that this personalisation was performed in the consumer's interest), while in reality what the insurance distributor, when setting the prices, takes into account is whether the device the consumer is using has a Microsoft operating system or macOS.[90] The objective of such a practice would be to artificially increase prices offered to consumers who are macOS users. One could argue that here a breach of GDPR and a misleading character of the market practice are just coincidental. Nonetheless, in virtually all scenarios where personalised pricing infringes on GDPR, the consumer

88 Howells, Twigg-Flesner and Wilhelmsson (n 80), 63.

89 Alexandre de Streel and Florian Jacques, 'Personalised pricing and EU law' in 30th European Conference of the International Telecommunications Society (ITS): 'Towards a Connected and Automated Society', Helsinki, Finland, 16th-19th June 2019 (International Telecommunications Society (ITS) 2019), 5.

90 Similar examples are indicated by Bourreau and de Streel (n 6), 3.

will be misled as to the price or how the price is calculated. This is because the price-related information that is provided to the insurance consumer may cause them to believe that all the data processing, performed within the price calculation, was lawful.

Moreover, a commercial practice shall also be regarded as a misleading omission within the meaning of Article 7 UCPD when a trader (insurance distributor) does not provide a consumer with all the material information necessary to make a well-informed decision and hereby causes or is likely to cause the average consumer to take a transactional decision that he or she would not have taken otherwise. In general, one can assume that information about the price and its personalisation is crucial for any consumer.[91] This is especially the case if the personalisation of price takes place using fully automated decision-making and a contract is concluded at a distance: in such cases Article 6(1)(ea) of the Consumer Rights Directive[92] might be applicable. Under this provision, a trader is obliged to inform the consumer in a clear and comprehensible manner that the price has been individually adjusted based on automated decision-making.[93] However, financial services are excluded from the scope of the Consumer Rights Directive since they are subject to comprehensive regulation in sector-specific acts at the EU level.[94] Yet remarkably, a provision on price personalisation, comparable to the one of Article 6(1)(ea) Consumer Rights Directive, cannot be found in the Directive 2002/65/EC concerning the distance marketing of consumer financial services.[95] Should one consider this legislative choice

91 Cristina Poncibò and Rossella Incardona, 'The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) 30 Journal of Consumer Policy, 31; *Fitness check of EU consumer law* (BEUC 2017), 5; *Ensuring consumer protection in the platform economy* (BEUC 2018), 9.

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

93 Rott, Strycharz and Alleweldt (n 21), 28–29. For a sceptical view of this provision, see Jabłonowska, Lagioia and Sartor (n 53), underlining that the impact of this provision may in practice depend on its interpretation, and the latter is disputed.

94 See Article 3(3)(d) Consumer Rights Directive, and contributions in Veerle Colaert, Danny Busch and Thomas Incalza (eds), European Financial Regulation Levelling the Cross-Sectoral Playing Field (Bloomsbury 2019); Golecki and Tereszkiewicz (n 86).

95 Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services [2002] OJ

meaningful, it would weigh against the interpretation that a failure to inform about the personalisation of insurance prices constitutes a misleading commercial practice under Article 7 UCDP.

Still, one could argue that – in the case of the personalisation of insurance prices – all the information that should be provided under GDPR should be regarded in the light of Article 7(5) UCPD as material within the meaning of Article 7(1) UCPD. A possible argument could run as follows: the provision of Article 7(5) UCPD suggests that information requirements established under EU law concerning commercial communications, including advertising or marketing, indicate what information should be considered material in this context. The catalogue of regulatory acts that should be taken into account is found in Annex II to UCPD. Given this list has merely a non-exhaustive, indicative nature, it is submitted that even though GDPR is not included in it, information obligations under GDPR should be considered material under UCPD. We argue that within the data-driven EU market economy, the relevance of data, including personal data, has been greatly increasing. Data has become a commodity, a factor shaping market strategies and behaviours.[96] These factual developments should be reflected by recognizing that data-related information obligations, such as those found in GDPR, form part of the core legal framework on mandatory consumer information under EU law. Under this view, the information duties that a data controller has to a data subject play an important role in shaping consumer digital literacy in the context of commercial communication including advertising or marketing. It follows that information obligations stemming from GDPR can be considered 'information requirements relating to commercial communication' including advertising or marketing within the meaning of Article 7(5) UCPD.

Further, one should consider the related question of whether an omission by a trader to provide information on the personalisation of insurance pricing causes or is likely to cause an average consumer to make a transactional decision that he or she would not have taken otherwise. In analysing

L 271/16. The EU legislator should, however, reconsider introducing the obligation to inform the consumer that the price has been individually adjusted based on automated decision-making in a clear and comprehensible manner also in the case of distance contracts for financial services. A revision of Directive 2002/65/EC is currently taking place.

96 The Geneva Association: Report Big Data and Insurance: Implications for innovation, competition and privacy (2018); Thouvenin, Suter, George and Weber (n 4), 227-230; Soyer (n 15), 166-167.

this question, one should point out that the personalisation of insurance prices, similar to the personalisation of prices on different markets, may lead to higher prices for certain consumers and lower prices for others. Consequently, some consumers may not want to purchase the product from a given trader in the knowledge that they can buy it cheaper from a different trader who does not personalise their prices.[97] Other consumers, for whom personalisation might result in paying lower premiums for the same insurance cover, may seek personalised offers. One could thus assume that a trader's omission to inform customers about the personalisation of insurance prices is likely to lead a consumer to make a transactional decision that he or she would not have made knowing that the price of the insurance product offered is determined in the process of digital personalisation.[98]

Moreover, what is interesting in the context of misleading omissions is that they are likely to coincide with GDPR infringements by a trader. Insurance distributors, who fail to inform insurance consumers that insurance prices are personalised, may also fail to ensure that consumers' personal data are processed in full compliance with GDPR. In particular, insurance distributors may omit to inform consumers as data subjects under GDPR about the specific purpose of personal data processing and the automated decision-making employed in the product distribution.

Assuming that a commercial practice passes the tests of Article 6 and 7 UCPD, it may still be subject to review as to unfairness under Article 5(2) UCPD, which serves as a safety net for consumers.[99]

Under Article 5(2) UCPD, which is labelled the general clause, a commercial practice shall be regarded as unfair if it is contrary to the requirements of professional diligence and it materially distorts or is likely to materially distort the economic behaviour (concerning the product) of the average consumer. The first question that should be answered in this context is whether the practice can be regarded as contrary to the requirements of diligence if it is based on processing personal data in a manner contrary to GDPR provisions. The requirements of professional diligence are understood as the standard of care that a trader may reasonably be

97 de Streel and Jacques (n 89), 5.

98 Introducing an explicit duty for traders to inform consumers about price personalisation and the main parameters used for the personalisation is recommended by Bourreau and de Streel (n 6), 11, with reference to OECD (2018).

99 Micklitz (n 80), 89; Stuyck, Terryn and van Dyck (n 79), 106; Howells, Twigg-Flesner and Wilhelmsson (n 80), 58.

expected to exercise towards consumers.[100] Traders who undertake activities that include the processing of personal data of consumers, including personalisation – or as in the case at hand: the personalisation of insurance prices – can reasonably be expected to comply with GDPR while processing that data. This implies that processing the personal data of consumers while infringing on GDPR requirements should be considered a commercial practice that is contrary to the requirements of professional diligence.

However, for a commercial practice to be regarded as unfair under Article 5(2) UCPD, further requirements must be met. In this context, it needs emphasising that not every (potential) distortion of consumer behaviour is automatically regarded as fulfilling the second premise of Article 5(2) UCPD. The distortion must be material, which means that a commercial practice must show sufficient impact to impair the consumer's ability to make decisions[101] and have the potential to affect the consumer's market behaviour. By contrast, insignificant instances of misconduct by traders do not qualify as leading to material distortions.[102] An informational advantage that traders necessarily have over consumers is not sufficient in itself to distort or have the potential to distort the average consumer's market conduct.[103] What is additionally required is an exploitation of the informational advantage by a trader (an insurance distributor) to the detriment of a consumer. Given the reality of digital mass-markets establishing whether personalising practices may materially distort consumers' behaviour may be difficult.[104]

100 Micklitz (n 80), 85; Howells, Twigg-Flesner and Wilhelmsson (n 80), 58-60.

101 Micklitz (n 80), 86–87. It is important to distinguish between an unfair commercial practice designed to influence a consumer's decision, basically leaving the consumer with no freedom of choice, and nudging, which is designed to induce a choice, but with a strong emphasis on full freedom of choice, see Avishalom Tor, 'The Critical and Problematic Role of Bounded Rationality' in Klaus Mathis and Avishalom Tor (eds.) *Nudging. Possibilities, Limitations and Applications in European Law and Economics* (Springer 2016), 4-7.

102 Hugh Collins, 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) 73 Modern Law Review, 101.

103 For more on the impact of new technology tools on the autonomy of contracting parties see Mik (n 2), 1-38.

104 Południak-Gierz (n 51), 172-173.

E. Infringement of GDPR as an unfair commercial practice?

The Chapter has so far discussed the interplay between GDPR and UCPD and spelt out typical circumstances in which an infringement of GDPR can be regarded as one of the factors leading to the unfairness of a commercial practice within which GDPR infringement occurred. In the next step, one could go even further and consider whether an infringement of GDPR itself could be considered an unfair commercial practice under UCPD. Recognising that an infringement of GDPR automatically justifies finding a commercial practice unfair under UCPD could substantially improve the legal situation of consumers who buy products as a result of personalisation practices and find that personalisation was executed without compliance with GDPR. Specifically, the consumer then could invoke remedies granted under Article 11a UCPD, i.e., claiming compensation, terminating the contract, or reducing the scope of their obligation.

The possibility of applying a similar 'shortcut' argument in order to ascertain one's rights was discussed in the CJEU *Pereničová* judgment.[105] There, the Court was confronted with the question of whether a finding that a commercial practice of using contractual terms that could mislead consumers as to the scope of their rights and obligations was unfair influences (or possibly even determines) the outcome of the assessment of whether these terms are to be considered unfair under Article 4(1) of the Unfair Contract Terms Directive (UCTD).[106]

The Court initially found that:

> 'A commercial practice such as that at issue in the main proceedings which consists in indicating in a credit agreement an APR lower than the real rate constitutes false information as to the total cost of the credit and hence the price referred to in Article 6(1)(d) of Directive 2005/29'.[107]

Based on the above finding the Court subsequently concluded that:

> 'A commercial practice such as that at issue in the main proceedings which consists in indicating in a credit agreement an annual percentage

105 Judgment of the Court (First Chamber), 15 March 2012, Jana Pereničová and Vladislav Perenič v SOS financ spol. s r. o., Case C-453/10, ECLI:EU:C:2012:144.

106 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.

107 Judgment of the Court (First Chamber), 15 March 2012, Jana Pereničová and Vladislav Perenič v SOS financ spol. s r. o., Case C-453/10, ECLI:EU:C:2012:144, para. 41.

> rate of charge lower than the real rate must be regarded as "misleading" within the meaning of Article 6(1) of Directive 2005/29/EC [...] in so far as it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise. [...] A finding that such a commercial practice is unfair is one element among others on which the competent court may, pursuant to Article 4(1) of Directive 93/13, base its assessment of the unfairness of the contractual terms relating to the cost of the loan granted to the consumer. Such a finding, however, has no direct effect on the assessment, from the point of view of Article 6(1) of Directive 93/13, of the validity of the credit agreement concluded.'[108]

The Court thus took the view that finding that a commercial practice of using a specific contract term meets the test of unfairness under UCPD is merely one of the factors to be taken into account in the assessment as to whether contract terms are at the same time unfair under the Unfair Contract Terms Directive. While the requirements provided under both the Directives in question should thus be examined independently of each other, the outcome of the assessment under the Unfair Contract Practices Directive retains relevance for the assessment under the Unfair Commercial Terms Directive.

Another issue is whether the same manner of reasoning should be applied when a term in a consumer contract is deemed unfair. As discussed above, one could assume that the inclusion of a such a term in consumer contracts should not automatically amount to an unfair commercial practice within the meaning of UCPD. Nevertheless, the unfair character of the contract term that is used by the trader should be considered when the fairness of a commercial practice (which includes using this contract provision) is assessed. This appears justified in cases where unfair contract terms in question do not meet the transparency requirement under UCTD. This is because it is the lack of transparency that makes the consumer prone to overlook a significant imbalance in the parties' rights and obligations created by the unfair term. It prevents the consumer from taking an informed transactional decision and, thereby, causes or is likely to cause the average consumer to take a transactional decision that he or she would not have taken otherwise.

108 Idem, para. 47.

Formally, the same approach should be applied in analysing the relationship between the Unfair Commercial Practices Directive and GDPR. It suggests that while a breach of GDPR should be considered an important factor when assessing the unfairness of a commercial practice under the Unfair Commercial Practices Directive, it does not, by itself, constitute an unfair commercial practice.

Further, a similar position in favour of the complementary character of the EU consumer protection provisions on the one hand and data protection provisions on the other hand was taken in the European Commission's Staff Working Document. There, it is claimed that the violation of data protection rules does not always mean that the practice would be regarded as unfair under UCPD, yet such data protection violations should be considered when assessing the overall unfairness of commercial practices under UCPD, particularly in the situation where the trader processes consumer data in violation of data protection requirements, i.e., for direct marketing purposes or any other commercial purposes such as profiling, personal pricing or big data applications.[109]

F. Conclusions

This Chapter aims at providing insights into the complex and yet unexplored interplay between GDPR and UCPD in the context of the personalised pricing of insurance products. As the law stands now, infringements of GDPR or the personalisation of prices (both in general and specific sectors) are not listed in Annex I to UCPD. The case, which the BEUC report makes for extending the blacklist of unfair commercial practices by including certain forms of infringement of GDPR, appears largely justified. Amendments proposed by BEUC would strengthen the protection of consumers' personal data since practices included in the blacklist are considered unconditionally unfair. Introducing such measures would be a particularly suitable response in cases where traders intentionally violate GDPR during personal data processing to be able to personalise the prices of insurance products.

109 European Commission (2016), Staff Working Document of 25 May 2016 on Guidance on the implementation/application of the Directive 2005/29 on Unfair Commercial Practices, SWD(2016) 163, 26.

Further, the Chapter has shown that there are cases of price personalisation of insurance products that do not comply with GDPR requirements and can be regarded as misleading commercial practices both under Article 6 and Article 7 UCPD. One should not regard such scenarios as being isolated and purely coincidental since misleading commercial practices that use personalisation are usually preceded by major GDPR breaches. Moreover, the analysis revealed several challenges posed by the automation of decision-making processes in product distribution within the insurance sector. Assuming that a similar level of protection should be granted to consumers both in financial services and other markets, one should recommend generalising the regulatory objective of Article 6(1)(ea) Consumer Rights Directive and imposing on traders the obligation to inform consumers about price personalisation when providing financial services, including insurance.[110] Tailored regulation of the information duties concerning automatic decision-making mechanisms requires a high degree of coherence between provisions on data protection, financial services, and consumer law.

Moreover, commercial practices undertaken in breach of GDPR can reasonably be seen as contrary to the requirements of professional diligence. However, for such practices to be regarded as unfair commercial practices under the UCPD, the assessment depends on whether the practice at hand also materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer.

Given the complexity of the subject matter herein analysed, and the evident digital vulnerability[111] of a contracting party who is both a consumer and a data subject under GDPR, one might be tempted to advocate a 'shortcut' solution, under which a breach of GDPR automatically constitutes an unfair commercial practice under the UCPD in cases of the personalised pricing of insurance products. A better view is to resist this urge and assume

110 See also Bourreau and de Streel (n 6), 11; OECD 2018; similarly Poncibò (n 7), 336.

111 Kasper Drazewski, *EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy*, (BUEC 2022) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf>: '… in digital marketplaces, most if not all consumers are potentially vulnerable. Instead of singling out certain groups of consumers, digital vulnerability describes a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, "datafied" consumer-seller relations and the very architecture of digital marketplaces'.

that the two regulatory regimes are independent but open for mutual influences.

Ideally, the extent to which insurance contracts can be personalised (individualised) should be determined by specific provisions of (insurance) law, preferably adopted following a public dialogue involving all stakeholders.[112] Determining which sectors of insurance should be governed by the principle of solidarity and which may be governed by the personalisation of insurance contracts will be a complex process needing time. For the time being, data protection law and consumer law will continue to play an important role in setting the limits for the market conduct of insurers.

112 Thouvenin, Suter, George and Weber (n 4), 243.

Let the Children Play. Smart Toys and Child Vulnerability*

Alessandra Pera, Sara Rigazio

A. Introduction

In the 1990s, children played with their toys asking questions and giving themselves the answers. Today, smart toys talk with the children through artificial intelligence and voice recognition systems, engaging in conversations and interacting with them, sharing stories and tailoring answers according to the kids' preferences. As a matter of fact, the extremely rapid technological advancement of recent years has abruptly affected also the children's entertainment sector, starting a completely new era.

Further confirming the growing importance and popularity of these new and revolutionary gaming instruments, in 2021 the World Economic Forum itself dedicated extensive research on this topic showing, indeed, that the trend is for the smart toy market to grow considerably over the years, increasing its market share by almost 200% from 2018 to 2023[1].

While smart toys' features offer undoubtedly exciting and educational opportunities, at the same time they raise several questions, mainly in terms of privacy, children's agency and market regulation, that all relate to the condition - concrete or potential, as further discussed below - of children's own vulnerability.

Therefore, this essay focuses on the concept of vulnerability and explores the vulnerable condition that arises from the use of these tools specifically in children belonging to the 5-10 age range group. This age range is the result of a precise methodological choice based on the two dimensions of this work, that are the taxonomy and the case-based one, respectively.

---

* This chapter is the result of a common research and reflection of the two authoresses. However, only within the scope of research evaluations, Alessandra Pera drafted Sections 2 and 3, while Sara Rigazio drafted Sections 4 and 5. The Introduction (section 1) and the conclusions (section 6) were co-authored.

1 Seth Bergenson, 'Smart toys: Your child's best friend or a creepy surveillance tool?' (*World Economic Forum*, 31 March 2021) <https://www.weforum.org/agenda/2021/03/smart-toys-your-child-s-best-friend-or-a-creepy-surveillance-tool/> accessed September 2023.

The first, relates to the multidimensional character and to the multifaceted factors of vulnerability that can vary, as we will explain in details, according to the context the individual is living in; the second, relates to the practical approach- that is necessary even if we work on taxonomies- linked to the case studies we analyze, that involve AI dolls and robots, quintessentially targeted at children-consumers of this age range.

In particular, through the analysis of two case studies, it shows some of the threats and the risks children can face, advancing some arguments on the possible alternatives and responses.

Whilst the concept of vulnerability is usually defined broadly as "the quality of being weak and easily hurt physically or emotionally"[2], referring to external risks, stress factors and circumstances within which an individual could be deprived of the capacity to self-determine and choose freely, we decide to employ a very exhaustive taxonomy that focuses on the different vulnerability's sources[3]. As we will explain in details, we apply the distinction between inherent and situational vulnerability, the first depending on intrinsic characteristics of the human nature, while the second mostly on the external setting. Through this distinction we can identify the sources of vulnerability in a specific case, making references to risk factors and highlighting their consequences.

The topic of smart toys shows, indeed, a multidimensional vulnerability often correlated within the context surrounding the kids. Consequently, our analysis engages with the intersectionality theory. As its leading thinker and scholar Kimberlé Crenshaw explains, various forms of inequality and oppression often operate together, exacerbating each other. To understand the real condition of the individual, then, it is necessary to look at the experience that the individual is going through, as a whole[4].

Such approach, therefore, will allow us to focus on the context-dependency of the personal experience of intersectionality including the inherent and the situational vulnerability: the single child or a specific type of vul-

2 See Oxford Dictionary, <https://www.oxfordlearnersdictionaries.com/definition/english/vulnerability?q=vulnerability> accessed September 2023.

3 Catriona Mackenzie, Wendy Rogers and Susan Dodds, 'Introduction: What Is Vulnerability and Why Does It Matter for Moral Theory?' in Wendy Rogers, Catriona Mackenzie & Susan Dodds (eds), *Vulnerability. New Essays in Ethics and Feminists Philosophy* (Oxford University Press, 2014) 1, 29.

4 Kimberlé Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination doctrine, Feminist Theory and Antiracist Politics' (1989) Un. Chi. Legal Forum 139.

nerable child might be individually exposed to many needs and restraints, meeting various social expectations, or dependent on limited material and social resources. While being exposed to a stable set of categorical (structural) interferences, the same child could encounter different forms of intersectionality within different backgrounds (i.e. inside the family, at school, at the hospital, in the religious community).

Within this framework, the response of the institutions, family and business operators, while noticeably complex, is equally necessary. Most importantly, we argue that the guiding principle of these actions must always stand for preserving and promoting the dignity of the person[5]. As we will try to foster through our analysis, the value of dignity represents the only and unique safeguard against the idea that the individual, and even more a child, represents solely an object and a source for data mining and collecting information.

Our paper is organized as follows: in the first part we will outline the concept of vulnerability by dwelling on the inherent-situational taxonomy referred to, continuing with the analysis of the two cases concerning smart toys and the issues underlying them, also with the support of the intersectionality theory. In the second part we will deal with the responses of the different actors involved to the concerns raised, suggesting that a child-centred approach, always oriented toward the fulfilment of the best interest of the child, not only is possible but imperative.

B. Vulnerability as a multidimensional concept

As Robert Chambers critically observed in his editorial of 1989[6], "Vulnerable and vulnerability are common terms in the lexicon of development but their use is often vague"[7]. Frequently confused with or used as a synonym of poverty or weakness, this author stressed instead the necessity and the opportunity of focusing on the effects vulnerability produces, that are the limitation or reduction of a person in her capacity, power or control to

5 See Stefano Rodotà, *Il diritto di avere diritti* (Laterza, 2015) 197.

6 Robert Chambers, 'Editorial Introduction: Vulnerability, Coping and Policy' (1989) 20 IDS Bulletin 1.

7 On the vagueness and the complexity of the term, see also Doris Schroeder, Eugenijus Gefenas, 'Vulnerability: Too Vague and Too Broad? (2009) (18) 2 Cambridge Quarterly of Healthcare Ethics 18.

protect her interests. From a biological or physiological perspective, then, vulnerability refers to a person's intrinsic characteristics and to a deficiency of means to manage without detrimental loss. In a social and relational length, therefore, vulnerability affects human being's access and effective exercise of fundamental rights and freedoms, undermining autonomy, curtailing individual capabilities or creating a sense of powerlessness[8].

In a similar perspective is the definition given by the UN Division of Social Policy and Affairs, which refers vulnerability to "a state of high exposure to certain risks, combined with a reduced ability to protect or defend oneself against those risks and cope with their negative consequences"[9].

As previously mentioned, we choose a different, specific approach to investigate vulnerability that is the one that takes into consideration and describes its different sources. Indeed, some authors[10] have proposed a very exhaustive taxonomy that distinguishes between inherent and situational vulnerability. The former, relies on the intrinsic characteristics of the human nature, connected to corporeality and dependent on others affective and social natures. The latter, instead, depends mostly on the external context and may be influenced by the personal, social, political, economic or environmental circumstances within which individuals or social groups live in, including oppression, domination and injustice. This last category stresses on inequalities of power, dependency, capacity or need, which could make a person vulnerable to harm or exploitation by others.

Inherent and situational vulnerability may be either dispositional (potential) or occurrent (actual). For example, considering our topic, minor children are dispositional vulnerable to digital technologies, but whether or not they will be actually harmed by them, it depends on a range of diverse factors, such as their age, capacity of understanding and consequently will and self-determination, level of digital literacy (personal and of the members of the family), level of education, family support, socio-economic status, their geographical location, the school infrastructures (material and human resources) and so on.

8 Martha Nussbaum, *Women and human development: the capabilities' approach* (Cambridge 2000). There are also scholars who criticise only negative association of vulnerability. For example, see Erin C. Gilson, *The Ethics of Vulnerability: A Feminist Analysis of Social Life and Practice* (New York and London Routledge 2016) 7, 8.

9 Division of Social Policy and Affairs, *Report on the world social situation, social and human rights questions: social development*, UN (United Nations), New York, 2001.

10 Catriona Mackenzie, Wendy Rogers and Susan Dodds, n 3 above.

As it becomes clearer, this distinction plays a crucial role since not only does it allow a more complete analysis of the specific situation of vulnerability at stake, but it also offers the opportunity to capture the peculiar side of the concept of vulnerability itself, i.e. its dynamic and layered dimension and nature. Moreover, this new framing is consistent with the recent critical advances in the vulnerability discourse that have criticized a static, stigmatized and categorical notion in favour of an alternative approach[11]. An interesting example is given by some policy documents from the European Commission in the matter of vulnerable consumers, where an evident change toward a new conception of vulnerability can be clearly observed[12]. Indeed, a new interpretation of the Commission recalls "that consumer vulnerability is situational, meaning that a consumer can be vulnerable in one situation but not in others, and that some consumers may be more vulnerable than others"[13]. Such a *dynamic* approach, therefore, can be reasonably deemed acquired in the broader theoretical vulnerability discourse[14].

11 One of the most prominent scholars who advances an alternative approach to vulnerability is Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2009) (20) Yale Journal of Law and Feminism, 23. In her vulnerability theory she employs the idea that "no individual can avoid vulnerability". See also Alison Cole, 'All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique' (2016) 17(2) Critical Horizons 260, 277; Gianclaudio Malgieri, Jędrzej Niklas, 'Vulnerable data subjects' (2020) 37 Computer Law & Security Review 105415; Lourdes Peroni, Alexandra Timmers, 'Vulnerable groups: The promise of an emerging concept in European human rights convention law' (2013) 11(4) International Journal of Constitutional Law 1056, 1085; Carol Levine et al., 'The Limitations of 'Vulnerability' as a Protection for Human Research Participants' (2004) 4 (3) The American Journal of Bioethics 44; Ryan Calo, 'Privacy, Vulnerability, and Affordance,' (2017) 66 DePaul L. Rev., 592.

12 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://commission.europa.eu/system/files/2018-04/consumers-approved-report_en.pdf.> accessed September 2023.

13 European Commission. (2016). Understanding consumer vulnerability in the EU's key markets. Factsheet, Brussels <https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet_en.pdf> accessed September 2023.

14 This approach has been employed also in the vulnerability assessment of refugees. In this respect, among others, see Daria Mendola, Alessandra Pera, 'Vulnerability of refugees: Some reflections on definitions and measurement practices' (2021) International Migration, 00, 1, 14.

Whilst Kate Brown and others pointed out, indeed, "the ubiquity and elasticity of [the term] vulnerability generates a sense of familiarity and common-sense or assumed understandings which conceals diverse uses with enormously varied conceptual dimensions"[15].

Accordingly, we shall now look at the specific case of the smart toys.

C. Smart toys

With the rise of the Internet of Things (IoT)[16], a growing number of households devices from television, security systems, to cooling and heating tools, are now able to perform a range of functions thanks to the Internet connectivity, sharing data[17]. Among them, toys have become part of the digital world as well, with the growth of the so called smart connected toys. Smart connected toys, or simply smart toys, are devices that encompass physical components of traditional toys connected to computer systems with online communication services. Given the fact that they can connect to mobile and cloud services, as well as to other smart toys, game consoles, tablets or smart phones, and also to underline how popular and widespread

15 Kate Brown, Kathryn Ecclestone and Nick Emmel, 'The Many Faces of Vulnerability' (2017) 16(3) Social Policy & Society 497, 510.

16 The term 'Internet of Things' is attributed to Kevin Ashton. See Kevin Ashton, That Internet of Things, RFID J. (June 22, 2009) <http://www.rfidjournal.com/that-internet-of-things-thing>. There is no universally agreed-upon definition, but generally, the term is used to describe networks of objects that are not themselves computers but have embedded components connected to the Internet. "Things" may include, for example, fitness trackers, personal vehicles, home appliances, medical devices, and even clothing used by individual consumers. The IoT potentially includes huge numbers and kinds of interconnected objects. In practice, IoT refers not to a simple or uniform network of objects but rather to a complex collection of objects and networks. See, Roberto Minerva, Abyi Biru, Domenico Rotondi, 'Towards a Definition of the Internet of Things (IoT)' (IEEE Internet Initiative, May 27, 2015), <http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf> accessed September 2023.

17 See Vivek Wadhwa, When the Toaster Shares Your Data with the Refrigerator, the Bathroom Scale, and Tech Firms, Singularityhub (June 30, 2015) <https://singularityhub.com/2015/06/30/when-the-toaster-shares-your-data-with-the-refrigerator-the-bathroom-scale-and-tech-firms/> accessed September 2023.

they have become in the recent years, some authors have even proposed the concept of the Internet of toys[18].

Recent reports have indeed confirmed that smart toys will represent an $18 billion software and hardware market by 2023, starting from an estimated $6 billion in 2018[19]. This increase is due mainly to the growing popularity, as mentioned, of smart-phones connected toys and related in-app purchases. In addition, another element to take into consideration is the flourishing market of educational smart toys, which grew exponentially especially during and after the pandemic and that now are often part of the schools' curricula[20].

Although there is no consensus regarding smart toy terminology, this phrase has long been used in the industry[21]. Consumers, usually, refer to smart toys in contrast with traditional toys such as puzzles or board games. The latest and most innovative examples are characterized by the direct interaction systems between the child and the toy, A.I. devices employed, image and voice processors and, of course, Internet connection through iOS or Android mobile applications.

As previously pointed out, the issues underlying the use of smart toys are several and diverse. In order to identify the profiles that we think affect and contribute mostly to the children's vulnerable condition, we decided to analyze two examples of recent marketed smart toys: *My friend Cayla* and *i-Que Intelligent Robot*.

I. The case studies

My friend Cayla and *i-Que Intelligent robot* are two Internet-connected toys, targeted to young girls and boys in the 5-10 age range, that talk and interact with children by capturing and recording children's communications

18 See, Wem-Nan Wang, Vivian Kuo, Chung-Ta King, Chiu-Ping Chang, 'Internet of Toys: An e-Pet overview and proposed innovative Social Toy Service Platform' *(2010) International Computer Symposium (ICS2010)*, Tainan, Taiwan, 2010, 264.

19 See Juniper Research (2018) <https://www.juniperresearch.com/press/smart-toy-revenues-grow-almost-200pc-by-2023> accessed September 2023.

20 Mariya Stoilova, Sonia Livingstone, Rana Khazbak, *Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes* (2021) *Innocenti Discussion Papers*, no. 2020-03, UNICEF Office of Research - Innocenti, Florence.

21 P.C.K. Hung, L. Rafferty, M. Fantinato 'Toy computing' in N. Lee (Ed.), *Encyclopedia of Computer Graphics and Games* (Springer Verlag 2019).

and by analyzing the recordings to determine the words spoken. They are both produced by Genesis Toys, a company based in California, which also markets and sells several other interactive toys and robots in the United States and abroad. In 2016 Genesis went under the scrutiny and was the object of an investigation by the Federal Trade Commission (FTC), as well as by the German Federal Network Agency and the Norwegian Consumer Council[22].

Specifically, Cayla and i-Que are made of two components: a physical doll and a companion mobile application.

The physical doll includes a Bluetooth microphone and a speaker and the companion app provides the data processing to enable the toy's ability to capture the private communications of children. Before playing with them, children are required to download the Cayla and/or i-Que application on a mobile device, to which the doll connects using Bluetooth technology. The companion apps are available from the Google Play and iTunes app stores.

Interestingly, the companion app for Cayla requests permission to access the hardware, storage, microphones and Wi-Fi connections, but fails to explain the significance of this permission. I-Que asks for access to the device camera even though the camera itself is not necessary to the robot's functionality and neither is explained to the users. Once the companion app establishes a Bluetooth connection, it connects the smart toys to the Internet. Cayla and i-Que record the conversations they have with the kids; moreover, the children's statements are converted into text that it is used to retrieve answers in Google or in Wikipedia.

Cayla and i-Que encourage children to converse openly with the toys, as if they were with a friend. According to the FTC's findings, Cayla was pre-programmed with many phrases that referenced to Disneyworld and Disney movies. For example, Cayla kept repeating that her favorite song was the one from the movie Frozen. And that she wanted to go to Disneyworld. This product placement was not disclosed so that parents were completely unaware of this in the conversations their child had with

22 See Federal Trade Commission, 6 December 2016, Genesis Toys and Nuances Communications <https://epic.org/wp-content/uploads/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf> accessed September 2023; Bundesnetzagentur removes children's doll "Cayla" from the market <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422> accessed September 2023; <https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws> accessed September 2023.

the doll. Similarly, i-Que was programmed to tell funny stories as well as scientific facts and to make strange sounds.

In addition, both Cayla and i-Que were programmed with a kid safe proprietary software, called Violet, designed to protect children from sensitive images or words that parents did not want the doll to use in front of their children. The Cayla companion app requires then a series of information to be set up: the kid's name, the parents' name, their favorite movie, their favorite meal, the name of the place where the kid lives, which school the kid goes to. Finally, Cayla explicitly invites children to set up their physical location in the general setting of the doll.

After some investigations, the FTC found out that Genesis did not comply with the general provisions regarding parental consent in order to collect, use or disclosure the personal information recorded in Cayla and i-Que[23] according to the Children's Online Protection Act (COPPA)[24]. Indeed, the company violated COPPA "by failing to make reasonable efforts to ensure parents receive direct notice of its information practices, including direct notice of any material changes to those practices"[25].

Consequently, as previously recalled, also Germany and Norway started investigating and, as a result, they banned Cayla and i-Que from the market.

In particular, the German Federal Network Agency classified Cayla as an "illegal espionage apparatus" so that retailers and owners could face fines if they continued to stock the toy or fail to permanently disable the doll's wireless connection. According to the Agency, indeed, "the toy can be used

23 See Federal Trade Commission, 6 December 2016, Genesis Toys and Nuances Communications, point n. 58 <https://epic.org/wp-content/uploads/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf> accessed September 2023.

24 Children's Online Privacy Protection Act, 16 C.F.R. This Act regulates the collection of children's personal information by operators of online services. It applies to operators of online services, websites, and apps directed to children under 13 as well as operators of online services, websites and apps serving a general audience. See Eldar Haber, 'The Internet of Children: protecting Children's Privacy in a Hyper-Connected world' (2020) (4) University of Illinois Review 1209. The bibliography on COPPA is evidently large. On the specific matter of processing children's data, also in a comparative perspective, see Milda Macenaite, Eleni Kosta, 'Consent for processing children's personal data in the EU: following in US footsteps?' (2017) 26 (2) Information & Communications Technology Law 146.

25 See Federal Trade Commission, 6 December 2016, Genesis Toys and Nuances Communications, point n. 97 <https://epic.org/wp-content/uploads/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf> accessed September 2023.

by anyone in the vicinity to listen in on conversations undetected". Moreover, the Agency started further investigation against the manufacturers on the ground that they violated also section 90 of the German Telecommunications Act, according to which "Objects must, by their form, purport to be another object or are disguised as an object of daily use and, due to such circumstances or due to their operation, are particularly suitable for intercepting the non-publicly spoken words of another person without his detection or for taking pictures of another person without his detection"[26].

The Norwegian Consumer Council as well looked at the terms and the technical features of Cayla and i-Que, finding a serious lack of protection of children's rights in general, and to privacy and security in particular[27]. Specifically, the report underlined the actual security flaws that, as documented, led already to an episode of hacking in 2015. Nevertheless, this episode was quickly dismissed by the company as an isolated event with no consequences for the marketing of the doll[28]. As a matter of fact, a series of technical tests performed by the Norwegian authority demonstrated that

26 See, Bundesnetzagentur removes children's doll "Cayla" from the market <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422> accessed September 2023.

27 Interestingly, beyond the most evident issues on privacy and security, the report underlined also that these smart toys encouraged and embody the actual debate on sexism. As a matter of fact, taking into consideration the three smart toys considered – My Friend Cayla, i-Que Intelligent Robot and Hello Barbie – "Hello Barbie is very interested in talking about clothes and toys, although she will also occasionally suggest career choices such as "politician". Cayla is happy to chatter about family, friends, and cooking, while the i-Que robot mostly steers the "conversation" toward science, lasers, and silly jokes". This aspect looks much more serious if we think that Cayla and i-Que come also with the option of simulating real conversation with the child. Finally, the Norwegian report reminded also that the Norwegian version of the app in Cayla banned words such as "homo- sexual", "bisexual", "lesbian", "atheism", and "LGBT". See <https://storage02.forbrukerradet.no/media/2016/12/toyfail-report-desember2016.pdf>, accessed September 2023, 35.

28 See '#Toyfail An analysis of consumer and privacy issues in three internet-connected toys', December, 2016 <https://storage02.forbrukerradet.no/media/2016/12/toyfail-report-desember2016.pdf> accessed September 2023. It is the report commissioned by the Norwegian Consumer Council, part of the larger project centering on the Internet of Things (IoT), that chose to analyze the three most popular smart toys available on the market at that time: My Friend Cayla, i-Que Intelligent Robot and Hello Barbie.

neither of the statements made by the manufacturer company about the security measures put in place to protect children, were true[29].

As it becomes clearer, Cayla and i-Que represent a vivid example of the risks and threats kids face when using smart toys without any control or compliance with the rules. The underlying issues, as we explained at the beginning, are diverse and concern multiple aspects such as the protection of privacy and the regulation mechanisms offered by the market. These issues, while peculiar in their specificity, still concur and can be traced to the concept of vulnerability, which, in the case we investigated, proves to be certainly multidimensional.

And as our analysis chooses and looks exactly to the dynamic and multifaceted notion of vulnerability[30], we apply now the taxonomy we have referred to before, to the concrete cases of Cayla and i-Que.

D. Case subsumption and use of taxonomies

Based on the taxonomy Mackenzie and others have proposed, and taking into consideration what we have underlined regarding the need to assume a dynamic approach on the vulnerability discourse, we can now argue that the phrase 'children between 5 and 10 years old are vulnerable when playing with smart toys', does not give any useful information.

Instead, we should argue that: being a child in the age range 5-10 years old makes you indeed *dispositional* vulnerable to diverse types of exploitation in the digital world (economic, sexual, psychological) and *occurrent* vulnerable if, as a matter of fact, Cayla or i-Que spied on you, recorded your voice, took your picture and your market preferences have been collected, shared and sold to other companies for profiling.

Once clarified this distinction, at the same time, the situational vulnerability becomes dispositional when the same child lives in a particular situation: for example, is left alone most part of the day, the only existing parent works and has no high level of education, also digitally speaking. The situational vulnerability, then, becomes occurrent if, for instance, a

29 See < https://storage02.forbrukerradet.no/media/2016/12/toyfail-report-desember2016.pdf> accessed September 2023, 32.

30 In this respect, see Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 International Journal of Feminist Approaches to Bioethics 121; Florencia Luna, 'Identifying and Evaluating Layers of Vulnerability – a Way Forward' (2019) 19 Developing World Bioethics 86.

family member gives the same child Cayla or i-Que as a gift and the child plays with it without any type of guidance or control for hours every day.

Applying this taxonomy clearly increases the variables concerning the vulnerability condition to consider, making it more difficult in some sense to identify and connect with each other the different sources of vulnerability. At the same time, tough, as the example clearly shows, it allows to recognize a peculiar situation of vulnerability distinguishing case by case (the child with no help from the family members from the child who, instead, lives in a situation where she has help and opportunities and is guided through the digital environment) and, most importantly, to decide and implement the right responses by the legal system and, in general, by the institutions[31].

Specifically in relation to the answers that can be given to erase or diminish the vulnerability's conditions, we believe that our analysis should also look at and could benefit from what Robert Goodin calls "pathogenic vulnerability"[32]. According to Goodin, this particular type of vulnerability depends on "all those morally unacceptable vulnerabilities and dependencies which we should, but have not yet managed to, eliminate". These are caused by prejudice or abuse in interpersonal relationships and by social domination, oppression, or political violence. The expression "pathogenic vulnerability" contributes to stress the attention on some institutional interventions, drafted to amend inherent or situational vulnerability, which, instead and in concrete circumstances, can have the paradoxical effect of increasing vulnerability[33].

In the case of children and smart toys is clear that all types of vulnerability co-exist: inherent and situational, occurrent and dispositional, with the risk of creating a pathogenic one. This is why we need also to consider the intersectionality theory.

---

31 In the matter of wrong responses by the institutions, see also Alessandra Pera, 'Il difficile bilanciamento tra tutela della madre vulnerabile, best interest del minore e diritti culturali della donna migrante al vaglio della Corte Europea dei Diritti dell'Uomo' (2021) (3) Comparazione e diritto civile 1179, where the author, retracing the case of a migrant woman whose daughters were given in adoption after she was considered unable to take care of them, suggests that, instead, a correct analysis of the woman's vulnerability, based on the taxonomy inherent/situational, could have prevented such a decision.

32 Robert E. Goodin, *Protecting the vulnerable: a reanalysis of our social responsibilities* (Chicago 1985) 203.

33 Catriona Mackenzie, Wendy Rogers and Susan Dodds, 'Introduction: What Is Vulnerability and Why Does It Matter for Moral Theory? 39.

As it is well known, the notion of intersectionality was originally conceived in the area of gender studies: Kimberlé Crenshaw used the metaphorical image of a car accident occurring at the crossroad of several streets or axes of discrimination to represent the sociocultural composition of underprivileged groups - in this case of black women - highlighting that inequality tends to be constituted by particular situations and contexts rather than by uniform class structures. In a famous article entitled "Demarginalizing the Intersection of Race and Sex"[34], the authoress describes the dynamics by which these two identity characteristics intersect with each other and the way in which their combination actually reinforces the subordination of black women.

What has to be underlined is that intersectionality is more than a mere sum of factors, in which one form of subordination is added to the other, as a sort of double oppression, mutually reinforcing each other; but represents a *combination* of factors that interact with each other, influence and determine each other without being able to be distinguishable anymore, causing further prejudice, beyond that caused by each singular form of subordination[35].

While there were preliminary uncertainties about the application of the theoretical premises of intersectionality in other disciplines different from the gender studies, and on the opportunity of taking into consideration additional axes or factors, such as age, ability, religion, and ethnicity[36], this theory has in fact gradually become established and widespread in Europe as well[37].

---

34 Kimberlé Crenshaw, 'Demarginalizing the intersection of race and sex: a black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics' (1989) cit; Kimberlé Crenshaw, 'Mapping the margins: Intersectionality, identity politics, and violence against women of colour' (1991) 43(6), Stanford Law Review 1241, 1299; Kimberlé Crenshaw, 'Twenty Years of Critical Race theory: Looking back to move forward', (2011) (43) Conn. L. Rev. 1253.

35 On the complexity that characterizes the concept of intersectionality, see Leslie McCall, 'The complexity of intersectionality' (2005) 30(3) Signs: Journal of Women in Culture and Society 1771. See also, Ann Phoenix, Pamela Pattynama, 'Intersectionality' (2006) 13 (3) European Journal of Women's Studies 187.

36 Mieke Verloo, 'Multiple Inequalities, Intersectionality and the European Union', (2006) 13(3) European Journal of Women's Studies 213; Knap 2008.

37 See Giovanni Marini, 'Intersezionalità: geneaologia di un metodo giuridico' (2021) (4) Rivista Critica del Diritto Privato 472, 475 who describes intersectionality as a 'travelling theory' for its capacity of being beyond the time and space dimensions and geographical borders. For this reason, the author suggests that it would be more useful not to consider intersectionality as a theory; rather, an approach.

For the purposes of our analysis, intersectionality becomes relevant where it represents an additional opportunity and a privileged tool for observing and, possibly, understanding better the vulnerability's condition. It is exactly in this perspective, then, that the context-dependency we referred to when analyzing the child - smart toy interaction, gets significance.

The common core linking the three different kinds of vulnerability distinguished above (inherent, situational and pathogenic) together with the approach of intersectionality is that they can explain the troubling sense of powerlessness, loss of control, loss of agency, which are common when we talk about vulnerability. Therefore, the discourse on vulnerability is enhanced with an additional element: *intersectional vulnerability*, giving (cross) relevance to the different and concurring factors of vulnerability and how they affect children; their treatment and the assessment of public and private remedies to reduce or exclude vulnerabilities' effects and intersectional harm. Such approach might be useful in evaluating the adequateness and efficacy of interventions drafted to improve the conditions of the children when using smart toys and to reduce their vulnerability.

E. Institutional policies and responses

It is within this 'new' framework that we have developed, that we now look at the issue of the responses and the choices that institutions and legal systems are called upon to make. Interesting examples of such responses in this respect are the UK Children's Code, the California Age-Appropriate Design Code, as well as the recent initiatives undertaken by the European Union.

The UK Age-Appropriate Design Code or Children's Code is a code of conduct issued by the Information Commissioner's Office in England[38], entered into force in September 2020[39] – the first of its kind - aimed mainly at information service providers who manage data for online services such

38 The ICO is the UK's independent body set up to uphold information rights. The principal task of this office is to uphold information rights in the public interest. Specifically, the ICO covers different subject' matters such as data protection, privacy and electronic communications, freedom of information, eIDAS regulation. The work of ICO includes also a dedicated priority to artificial intelligence. See < https://ico.org.uk> accessed September 2023.

39 The Code was issued on 12 August 2020 and came into force on 2 September 2020. As stated in the Code, providers should bring their processing in line with the standards in this code by 2 September 2021. See, <https://ico.org.uk/for-organisations/guide-to

as apps, games, websites and social media that minors are *likely* to access. This code provides for a group of 15 standards that are defined as "a set of technology-neutral design principles and practical privacy features".

Part of these standards concern the personal interaction between the child and the technological tool: indeed, we find the standards regarding the data protection assessment, the fulfillment of the best interest and the default setting. The rest of the standards provided are more focused on aspects related to the functions of the technological tool and the potential harms that could derive from it.

As a matter of fact, we find the geolocation, the profiling, the data sharing standards and the part related to the smart toys. In this respect, the code offers interesting and straightforward guidance to business operators since it clearly requires that the types of data that will be processed by the smart toy (personal and family member's information for example) when connected to the Internet, is fully disclosed in advance[40]: this means, in practice, helping to create the conditions in order to avoid or, at least, to limit the possibilities of occurrent vulnerability to happen. Furthermore, when the code requires that this disclosure of information should take

-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/transitional-arrangements/#code2> accessed September 2023.

40 See standard n. 14 of the Code and the guidance <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/14-connected-toys-and-devices/> accessed September 2023. Also, in this respect, the idea of acting 'before' refers to the 'design thinking'. Since it was first used in the context of organizations, the 'design' term has over time taken on different nuances and traits depending on the context in which it was employed. The idea behind this new approach is to put the person, who may be the user of a good or service or the recipient of a decision, at the center. Scholars from different disciplines have then gradually tried to apply it in many diverse areas of interests, including the legal context. Without any attempt to be exhaustive, see Batya Freedman, considered the leading scholar in the value sensitive design, David G. Hendry, Batya Friedman, 'Value sensitive design as a formative framework', Ethics and Information Technology, 2021, 23, 39, 44; Helen Nissenbaum for the responsible design, Lucas D., Introna, Helen Nissenbaum, 'Shaping the Web: Why the politics of search engines matters', The Information Society (2000) 16, 3, 169; Lee A. Bygrave for privacy design related issues, 'Security by Design: Aspirations and Realities in a Regulatory Context', Oslo law review (2021) 8, 3; Ann Cavoukian, Privacy by Design: The 7 Foundational Principles, <https://www.ipc.on.ca/wp-ontent/uploads/Resources/7foundationalprinciples.pdf> accessed September 2023; Margareth Hagan, Law by design <lawbydesign.co> accessed September 2023; Lina Jasmontaite et al., 'Data Protection by Design and by Default', (2018) 4 European Data Protection Law Review 168.

place "just in time" and be facilitated through interactive messages with the user, this means also to intervene on the situational vulnerability when it could turn on to dispositional /occurrent. In the example we made above, applying the taxonomy to the child who lives in a particular disadvantaged situation in terms of lack of instruments available, the fact that all the information regarding the data processing is given in advance at the moment of the purchase, and also during the use of the smart toy, can evidently diminish the possibilities of her vulnerability.

Moreover, there is another aspect that deserves to be emphasized and it is the fact that the overall structure of this code fully reflects the rationale behind the UN Convention on the rights of the child[41], not only where it explicitly mentions it, but where the entire framework is an expression of it. As it is indeed stated, the code aims to protect the child *within* and not *from* the digital dimension[42]. This means that the code has made as its own the fundamental principle that the child, an active subject in the digital realm and in the legal system, should be recognized, according to the level of maturity demonstrated, gradual autonomy[43]. In relation to vulnerability,

41 A/RES/44/25. The U.N. General Assembly approved the Convention on the Rights of the Child (CRC) on 20 November, 1989, in New York. The Convention entered into force on 2 September 1990. Nowadays, it is the most recognized and ratified international document, with the sole exception of the United States of America. The text of the Convention is available on the U.N. website at <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> accessed September 2023. For a general overview on the UN Convention, see Phylip Alston, J Tobin, *Laying the foundations for Children's rights* (Innocenti UNICEF 2005); Rachel Hodgkin, Peter Newell, 'Implementation handbook for the Convention on the Rights of the Child' (Innocenti UNICEF 2007); D. McGoldrick, 'The United Nations Convention on the Rights of the Child' (1991) 5 International Journal of Law and the Family 132.

42 See the executive summary of the UK Children's Code, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/executive summary/ accessed September 2023.

43 The reference is to art. 5 of the UN Convention on the Rights of the Child according to which *States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention".* Particularly relevant, even tough written in a complete different setting where the digital dimension was still far away, the words by Gerison Lansdown, *The Evolving Capacities of the Child* (Innocenti UNICEF Firenze 2005): "*Action is needed in law, policy and practice to promote cultural change in which the contributions children make and the capacities they hold are acknowledged" e, ancora, "[…] the*

this reinforces, in turn, the idea that the context-dependency perspective (i.e. the gradual autonomy), is able to catch the dynamic essence and the in-progress nature of vulnerability itself, taking into consideration all the different possibilities according to the taxonomy we have explained.

Imitating the model of the UK Children's Code is the California Age-Appropriate Design Code (CAADC)[44], approved on September 15, 2022 by the California Assembly[45]. The CAADC is modelled after the UK Children's Code and it also targets primarily all services on line that are *likely* to be used by minors. Interestingly, the CAADC recalls the concept of the best interest of the child many times in the text. This seems quite remarkable considering that the United States is the only country that has not ratified the UN Convention yet[46].

The European Union has also shown a growing interest and commitment to the issue of children's protection in the digital environment in general. It should, moreover, be noted that as early as 2012 the Commission launched the "Better Internet for kids – BIK+" initiative, which consisted of a real strategy of action on four main guidelines, concerning: the quality of online content aimed at minors, the awareness and subsequent empow-

---

most critical challenge is to create a better dialogue between adults and children about how the adult world can meet its responsibilities to fulfil, respect and protect children's rights". See, also, Sheila Varadan, 'The Principle of Evolving Capacities under the UN Convention on the Rights of the Child, (2019) (27(2)) The International Journal of Children's Rights 306.

44 AB2273 California Age-Appropriate Design Code, to entry into force on July 1st, 2024, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

45 At present, it is worth recalling that on September 18, 2023 a federal judge granted a preliminary injunction in favor of NetChoice, saying that the California Age-Appropriate Design Code violates the First Amendment. The rationale behind the decision lies in the fact that the law would force web sites to erect barriers on children and adult alike. In particular, the judge contested that the age verification method could involve invasive technology like face scans or biometric information. The motion was presented by NetChoice, a national trade association of online businesses whose members include, among others, Big Tech. The judge affirmed that NetChoice is likely to prevail on its claim that the CAADC violates First Amendment, so that the law cannot be enforced. At the moment, the State could still appeal the injunction. Nevertheless, the draft of the CAADC could serve as a roadmap for the future.

46 The reasons behind the missing ratification of the UN Convention on the Rights of the Child by the USA are multiple and diverse and they would go beyond the scope of this paper. For an overview on this matter, see the interesting analysis by Silvia Sonelli, 'I Children's Rights nel diritto statunitense tra Costituzione e Convenzione mancata', (2019) 3 Rivista Critica del Diritto Privato, 415.

erment of minors themselves, the creation of a safe digital environment and, finally, the fight against sexual abuse and the dissemination of child pornography online[47]. Since 2012, there have been many other projects, which have also gone hand in hand with as many legislative changes within the Union, by the EU institutions, at the forefront of child protection.

As a matter of fact, the 2012 BIK+ strategy was updated in 2022 in light of the imminent passage of the Digital Services Act and the commitment made in the proposed regulation on the European Digital Identity (EDi)[48]. Similarly, the European Data protection board's guidelines on data relating to children, expected soon, as announced in the work program 23/24[49], will also be relevant. Of all the initiatives, certainly the most significant in terms of our topic is the one concerning the establishment of a working group for the draft of the European age-appropriate design code. In December 2022, as a matter of fact, a call was launched to identify the members of this group that will have to draft the code by early 2024. The project certainly represents an important step by the EU institutions in the intended and shared direction, as already seen at the international level in the British and US experiences, of the protection of minors' vulnerability in the digital environment, in a context, tough, where the action required concern the diverse factors of vulnerability.

In this respect, the successful reception of the UK Children's Code model could be enlisted in the phenomenon of the circulation of legal models[50] and, therefore, albeit in a future perspective, of legal transplants. Without

47 COM (2012) 196, online on https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196.

48 COM(2021) 281 final, online on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281, amending Regulation (EU) No 910/2014.

49 See, https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf.

50 Generally, on the phenomenon of the circulation of legal models, see Alan Watson, *Legal transplants: an approach to comparative law* (Edinburgh, 1974); Alan Watson, 'Law and legal change' Camb. L. J. (1978) 38, 313.; Alan Watson, 'TwoTier Law, an approach to law making' Int. & Comp. L. Q. (1978) 552; Alan Watson, 'Legal change: sources of law and legal culture' Un. Of Pennsylvania L. Rev. (1983) 131, 1121. With some criticisms on Watson theory, see Otto Kahn-Freund 'Book Review, Legal Transplants' L.Q.R. (1975) 91, 292; William Twining, 'Diffusion of law: a global perspective' Journal of Legal Pluralism (2004) 49, 1, 34, 35; William Twining, 'General jurisprudence: understanding law from a global perspective' (Cambridge University Press London 2009); Pier Giuseppe Monateri, *The 'Weak Law': Contaminations and Legal Cultures (Borrowing of Legal and Political Forms)*, 2008, available on line at the Alan Watson Foundation website: <www.alanwatson.org> accessed September 2023.

claiming to delve into such a far-reaching topic, we simply observe that, as in the case of other phenomena, for example in the environmental matters[51], also for the issue of children's vulnerabilities in the digital environment, and so in the case of the smart toys, the acquisition of already established models could facilitate the achievement of reform goals.

Moreover, as proven by the data on the market growth in the sector, smart toys have already conquered a significant share in the economy with a global dimension. Therefore, we can easily recognize that this is a mutual and shared matter, that appear common in the globalized world, and not, instead, strictly linked to a particular cultural, social or legal background.

A further confirmation in this regard also comes from the General Comment n. 25 of 2021 by the Committee[52] on the Rights of the Child, devoted precisely to the protection of the child in the digital environment[53].

On legal formants and circulation of models, see again Rodolfo Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law' The American Journal of Comparative Law (1991) I, 39, 1, 34 and II, 343; Rodolfo Sacco, Antonio Gambaro, *Sistemi Giuridici Comparati* (Utet Torino 1996) 4; Rodolfo Sacco, *Introduzione al diritto comparato* (Utet Torino 1992) 43; Rodolfo Sacco, *Circolazione e mutazione dei modelli giuridici*, Digesto civ., II, Utet, Torino 365.

For the dialogue between Rodolfo Sacco's and Alan Watson's theories, see Silvia Ferreri, 'Assonanze transoceaniche. Tendenze a confronto' Quadrimestre, rivista di diritto privato (1993) 1, 179; Ugo Mattei, 'Why the wind changed. Intellectual leadership in western law' Am. J. Comp. Law (1994) 42, 195; Alan Watson, 'From legal transplants to legal formants' American Law Journal of Comparative Law (1995) 43, 3, 469; Pier Giuseppe Monateri, 'Black Gaius' Hastings L.J. (2000) 51, 510.

51 On the specific matter of environoment, see Barbara Pozzo, "Modelli notevoli e circolazione dei modelli giuridici tra in campo ambientale: tra imitazione e innovazione" in *Studi in Onore di Antonio Gambaro. Un giurista di successo* (Giappichelli 2017).

52 The Committee is a body of 18 independent experts that monitors the implementation of the U.N. Convention on the Rights of the Child and of the two Optional Protocols to the Convention, by the State parties. In addition to this monitoring work the Committee publishes its interpretations on the content of human rights provisions, known as general comments, on specific matters. In these comments the Committee makes recommendations on thematic issues related to children that the State parties should dedicate more attention to, in terms of legislative and regulatory measures to adopt or improve.

53 See CRC/C/GC/25 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation accessed September 2023. In the matter of the protection of children in the digital environment the literature is very rich. Among the others, see Alessandro Mantelero, 'Children Online and the Future EU Data Protection Framework: Empirical Evidences and Legal Analysis' Int. J. Technology Policy and Law (2016) 2, 169; Lina Jasmontaite, Paul de Hert, 'The EU, Children under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the

The final text of the Comment is the result of a series of initiatives aimed at investigating the relationships between children's rights and the digital environment in the light of the rights recognized in the U.N. Convention. Specifically, the Committee received inputs in 2019 and in 2020 from State parties, regional organizations, stakeholders and, most importantly, from children[54].

The key elements of this document lie in the method by which it was drafted and the recipients to whom it is addressed. Regarding the method employed, as mentioned above, the comment is made of the observations coming from different actors. The most relevant part comes from the children: from 27 countries and different socioeconomic backgrounds, they are, therefore, the real protagonists, in full accordance with the essence of the rights recognized in the Convention. The concept of participation as one of the instruments for the child to affirm his or her own rights, and

Internet' International Data Privacy Law (2014) 5, 20; Eva Lievens, Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation', Computer Law & Security Review (2018) 34, 2, 269; Simone van der Hof, 'I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World', Wisconsin International Law Journal (2017) 34 (2) 409; Simone van der Hof, Eva Lievens, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR', Communications Law 23 (2018) https://papers.ssrn.com/abstract=3107660 accessed September 2023; Esther Keymolen, Simone Van der Hof, Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust, Journal of Cyber Policy, (2019) 4:2, 143-159; Francesca Ippolito, '(De)Constructing Children's Vulnerability under European Law' in Protecting Vulnerable Groups, The European Human Rights Framework (Bloomsbury Publishing 2015) 23; Gary T. Marx, Valerie Steeves, 'From the Beginning: Children as Subjects and Agents of Surveillance', (2010) 7(3/4), Surveillance & Society 192; Ellen McGinnis et al., 'Giving Voice to Vulnerable Children: Machine Learning Analysis of Speech Detects Anxiety and Depression in Early Childhood,' (2019) IEEE Journal of Biomedical and Health Informatics, 1; Louise Holly, 'Health in the Digital Age: Where Do Children's Rights Fit In?', (2020) 22, 2 Health and Human Rights Journal 49; Simone van der Hof et. al., 'The Child's Right to Protection against Economic Exploitation in the Digital World', (2020) 28 International Journal of Children's Rights 833; Simone Van der Hof, *Children and data protection from the perspective of children's rights - Some difficult dilemmas under the General Data Protection Regulation* (Wolters Kluwer: Belgium 2018).

54 See, Amanda Third, Lily Moody, *Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25*, 2021 (London and Sydney: 5Rights Foundation and Western Sydney University) <https://5rightsfoundation.com/uploads/OurRIghtsinaDigitalWorld-FullReport.pdf> accessed September 2023.

as a duty for the other actors (states, businesses) to fully comply with the obligations of the U.N. Convention, is indeed at the base of the new concept of the child the Convention is expression of: an active subject with rights (and duties), and not a mere object of someone else's decisions and choices.

This approach moreover might reduce the risk of pathogenic vulnerabilities and ineffective institutional responses.

The recipients identified are the States parties but, also, parents and caregivers, civil society such as organizations working in the field of children's rights and in the field of the digital environment, and businesses. All the actors are required to meet a series of obligations not only to protect children from any potential harm in the digital environment, but also to *prevent* those harms through monitoring activities and child-rights impact assessments. This is possible due to the intrinsic strength and yet innovative side of the U.N. Convention, which is to *foresee* the protection of children also by private actors.

Regarding specifically the topic of vulnerability, recalling what we have established through the taxonomy we proposed, we can easily recognize that, if adequately addressed and acknowledged (also) in advance, situational or occurrent vulnerabilities can be avoided or limited. In this respect, therefore, the participation element plays a crucial role[55].

Another response, even if a different level, can be found also in the recent initiative of the *supported decision-making* (SDM) agreement[56], an instrument that puts the individuals' needs at the center, without depriving the subjects of their agency but, at the same time, assisting them in their choices. In the last few years this instrument has gained increasing attention in the public debate in the United States, in particular after the landmark

55 For the matter of participation related to vulnerable persons in the decision-making process, see Latifa Jackson et al., 'Including Vulnerable Populations in the Assessment of Data From Vulnerable Populations' Frontiers in Big Data 2 (June 28, 2019): 7 <https://doi.org/10.3389/fdata.2019.00019> accessed September 2023.

56 The *supported decision-making* (SDM) agreement allows people with disabilities to retain their decision- making capacity by choosing trusted advisors, such as friends, family members, or professionals, to serve as supporters in every day life's choosing. For a brief and practical overview see, https://www.aclu.org/wp-content/uploads/legal-documents/faq_about_supported_decision_making.pdf accessed September 2023; among scholarly writing see, Karrie A. Shogren, Michael L. Wehmeyer, Jonhathan Martinis, Peter Blanck, *Supported Decision-Making: Theory, Research, and Practice to Enhance Self-Determination and Quality of Life* (Cambridge University Press 2018).

decision in *Ross and Ross v. Hatch*, that reaffirmed an individual's right to choose how to live with the support needed in the community[57].

The declared aim of SDM, indeed, is to empower people to make their own decisions, to the maximum extent possible, to increase their self-determination. Mostly, SDM is seen as a valuable alternative to the traditional overly restrictive instruments of guardianships or substitute decision making regimes, to which usually certain categories of people (for example mentally or cognitive disabled people or older adults) have been relegated to by the law so far[58].

The key element of SDM is, therefore, the protection of the person at her highest expression, namely, self-determination which is what leads people to live *meaningfully* their life in a certain community. And it is exactly in this perspective that we see the connection with vulnerability and, in particular, with the case of children's vulnerability and the use of smart toys.

F. Ways forward and conclusions

What we have tried to do in these pages is to explore how the concept of vulnerability could be declined in the specific situation of children playing with smart toys and what coordinates – if any – we could identify to avoid or, at least, limit that situation of vulnerability. The risks and the threats that we acknowledged led our analysis to look for the reasons behind those risks but, mainly, for the responses that legal systems and institutions have already given or, possibly, could still give.

One fundamental element that is critical to underline is that the answers we considered, namely the UK and the California Age-Appropriate Design Codes, as well as the EU initiatives together with the *supported decision-making agreement*, are not pathogenic responses. According to what Goodin says, as a matter of fact in this specific case, these are all *pro-active*

57 *Ross and Ross v. Hatch*, Case No. CWF-120000426 (Circuit Court of Newport News, 2013). Some of the material can also be found at <https://jennyhatchjusticeproject.org/justice-project/trial-information/> accessed September 2023.

58 See Anna Arstein-Kerslake, 'An empowering dependency: Exploring support for the exercise of legal capacity' (2016) 18(1) Scandinavian Journal of Disability Research 77; Anna Arstein-Kerslake, Michelle Browning, Joanne Watson, Jonathan Martinis, Peter Blanck, 'Future directions in supported decision making' (2017) 37(1) Disability Studies Quarterly; Peter Blanck, *eQuality: The struggle for web accessibility by persons with cognitive disabilities* (Cambridge University Press 2014).

proposals that, implicitly or explicitly, recognize the necessity to distinguish the actual or potential situations of vulnerability and try to fill in the gaps, practically (establishing the set of standards in the codes and with the support of the community in the SDM).

It is true that there are still many Caylas and i-Que Robots on the global market, also because e-platforms make it possible to sell repeatedly world widely even products not 'officially' on the market anymore.

At the same time, tough, there is also Roybi Robot, the 2021 winner of the Smart Companion category in the Smart Toy Awards, the event organized by the World Economic Forum in collaboration with UNICEF and its AI for children project[59], together with some companies such as PWC, Dell tech and the University of Berkley. The aim of this event was to find the most promising smart toys for children that promoted safe, trustworthy, ethical, and responsible use of AI. The idea is to encourage the use of technology to increase and improve the enormous potential and opportunity in education that these tools could bring with them.

Roybi represents precisely the example of how smart toys can actually be a source of safe learning, safe design and conscious use for the children. Indeed, beyond providing kids with a private tutoring experience that uses Artificial Intelligence, Roybi Robot introduces them to technology, math, science, and multiple languages**.** This smart toy explicitly refers to age-appropriate design features, is considered 'child-friendly A.I.' and indeed provides educational content[60]. Finally, Roybi's award is the result of the evaluation of experts and children: this confirms, once again, that participation and, mostly, participation by the subjects who should be the final user (potentially, at least, vulnerable users) is essential.

In this respect our analysis pointed out that the vulnerability condition of children in the digital environment, when using smart toys, needs to be declined taking into consideration: the taxonomy we described regarding the inherent/situational and dispositional/occurrent distinction and the

59 The Office of Global Insight and Policy is leading a two-year project to better understand how Artificial Intelligence (AI) systems can protect, provide for, and empower children<https://www.unicef.org/globalinsight/featured-projects/ai-children> accessed September 2023. UNICEF worked together with the Government of Finland, and collaborated with the IEEE Standards Association, the Berkman Klein Centre for Internet & Society, the World Economic Forum, the 5Rights Foundation and other organizations.

60 About the innovative features of this smart toy, see <https://roybirobot.com> accessed September 2023.

principles of the Convention on the rights of the child, namely the best interest and the evolving capacities of the child.

In this perspective, the result we get is in accordance with the very essence of childhood itself: being in progress, *in fieri*. This is the reason why we chose to employ that specific type of taxonomy on vulnerability together with the intersectionality approach. As we argued at the beginning that the ultimate goal must always be the promotion and the protection of the human dignity, the case of smart toys showed how easy it is to deviate from this goal, if all the actors involved do not pay enough attention and do not commit to this aim[61]. The risk is that what Rodotà[62] called "corpo elettronico" - that is all the information that make our identity - could not be reunited with the "corpo fisico". This is, instead, where the value of dignity becomes *the* critical element: it avoids that the person becomes just a source for profiling, selling data or an object of surveillance.

Institutions and civil society, then, have a precise responsibility towards the rest of the community in guaranteeing that this will not happen and to put in place actions that actually empower people, reducing or eliminating their vulnerability, not simply eliminating the problem, as in the case of Cayla and i-Que, that were just removed from the market.

As the case of smart toys have clearly demonstrated, the empowerment of children not only is possible but could represent a valid and appropriate

61 On the matter of responsibility, and in particular on the necessity for the institutions of taking a straightforward position, particularly interesting is the testimony that Prof. Woodrow Hartzog, from Boston University School of Law, gave on September 12, 2023 during the hearing, before the US Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, on "Oversight on A.I.: Legislating on Artificial Intelligence". Prof. Hartzog stressed the point that the policy-approaches of the last few years, tough significant, are not enough. He then stated that "To bring AI within the rule of law, lawmakers must go beyond half measures to ensure that AI systems and the actors that deploy them are worthy of our trust". He also underlined that "trust and relational vulnerability are the critical lenses through which to view issues of privacy, data protection, and civil rights in the digital age". The text of the testimony is available at <https://www.judiciary.senate.gov/imo/media/doc/2023-09-12_pm_-_testimony_-_hartzog.pdf> accessed September 2023. See, also, Solon Barocas, Andrew Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671; Andrew Selbst, Solon Barocas, 'Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law' (2023) 171 University of Pennsylvania Law Review 1023; Woodrow Hartzog, *Privacy's blueprint the battle to control the design of new technologies* (Harvard University Press 2018); Woodrow Hartzog, 'Unfair and Deceptive Robots' (2015) 74 Mar. L. Rev. 785.

62 See Stefano Rodotà, *Il Diritto di avere diritti* (Laterza 2016), 197.

suggestion to limit their vulnerability. Making the children more digitally literate[63] - their selves or through the intervention of their parents or guardians or agreed supervisor, in the case of the supported decision-making agreement - much more aware of their rights and, finally, realize what should always be the ultimate goal: pursuing their best interest.

63 See, also, the initiatives recently taken by the Italian data protection authority that aim at protecting minors online through an intense activity of dissemination about the digital environment. Particularly relevant the last publication by one of the members of the Authority, Agostino Ghiglia, of the book entitled *Educazione Civica Digitale* (Roma, 2023). More generally, on the commitment of the Authority, see <https://www.garanteprivacy.it/temi/minori> accessed September 2023.

Standards to Face Children and Patients Digital Vulnerabilities

Denise Amram

A. Introduction: digital vulnerabilities and the digitization of vulnerabilities

The advent of the digital era has strongly impacted on the way people lead their daily lives. In fact, novel contexts where diverse cultures, needs, and values intersect with the potential of data-driven economy, where individuals can be exposed to a series of new risks, or be included in minorities due to a combination of factors that affect their life and existence at a particular historical moment. The digital transformation of services, products, and relationships impacts on the mechanisms for fundamental rights protection, enforcement, and empowerment. This is because new risks have emerged (and are still emerging) in the digital environment, leading to what is referred to as "digital vulnerabilities". For example, cybersecurity profiles or issues related to interoperability requirements are proper only of the digital dimension, shaping additional assessments and consequent measures to be implemented exclusively to protect fundamental from specific risks emerging online or from the operations set by new technologies.

In addition to the digital vulnerabilities, within the cyberspace already known risks may require additional safeguards compared to the ones implemented to face the same ones within the physical dimension. For example, in the healthcare sector, the patient is still vulnerable because of the information asymmetry in providing consent to healthcare choices, however, where digital technologies that are supporting diagnosis, treatment, or rehabilitation activities, might change the results of the impact assessment. Therefore, new methodologies and different risk mitigation measures shall be adapted considering the process of "digitalization of vulnerabilities", as a supplementary ground to be properly addressed by the relevant stakeholders to protect and promote fundamental rights also in the digital dimension.[1]

1 D.J. Solove, *The New Vulnerability: Data Security and Personal Information, in Securing Privacy in the Internet Age*, Radin & Chander, eds., Stanford University Press, 2008,

The impact of the digital dimension on fundamental rights generally relates to the analysis of the effects that the potential lack of transparency or awareness has on the individuals, especially as far as the data processing activities (such as profiling of habits or behaviours, or the secondary use of data) are concerned. In fact, the gradual loss of control over the flow of information in the digital environment is the main issue to be addressed in order to avoid negative implications from data sharing. In particular, what should be subjected to assessment is the increasing probability to suffer negative consequences, including unforeseeable ones, from the processing of personal (and non-personal) data in the digital dimension. [2] Among the most common scenarios in this regard, there is the necessity to address possible unauthorized access to information concerning the individual, as well as the unauthorized profiling of the individual habits, resulting in direct (or indirect) exposure to automated content or decisions for purposes not necessarily related to the ones that led to the original data collection. [3]

The interest on this topic arises from the number and relevance of the legislative initiatives promoted within the framework of the European Union's strategy on data and the digital market.[4] They all share a common approach based on risks analysis: in fact, they are all structured to identify roles and responsibilities among the various actors in a specific data flow, in order to better identify and assess the potential impact on users, both

GWU Law School Public Law Research Paper No. 102 <https://ssrn.com/abstract=583483>.

2 A. Mantelero, M.S. Esposito, *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, in *Computer Law & Security Review*, Volume 41, 2021, 105561, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2021.105561>.

3 G. Comandé, *Regulating Algorithms' Regulation? First Ethico-Legal Principles, Problems, and Opportunities of Algorithms*, in T. Cerquitelli, D. Quercia, F. Pasquale, *Transparent Data Mining for Big and Small Data*, *Springer*, *2017*, 169 ff.

4 Regulation (EU) 2016/679 of the European Parliament and ft he Council of 27 April 2016 on the protection of natural persons with regard ft he processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Digital Service Act, Regulation (EU) 2022/2065 of the European Parliament and ft he Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), the Regulation (EU) 2022/868 of the European Parliament and ft he Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance); Proposal for a Regulation ft he EU Parliament and ft he Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final, etc.

as individuals and as categories of vulnerable subjects. As a consequence, diversified compliance levels with specific obligations aim at protecting users (*ie* the recipients of the service or product being marketed, or the data subject of the data processing activities) from different perspectives. Examples of such obligations include the data protection impact assessment under Article 35 of EU Regulation n. 2016/679 (hereinafter GDPR) [5], the evaluation of the reliability of systems based on artificial intelligence techniques under the recently approved EU Regulation 2024/1689[6], or the obligations of due diligence on online content imposed by the EU Regulation n. 2022/2065 on Digital Services Act (hereinafter DSA)[7].

This contribution aims to provide insights into the methodology to be applied for analyzing the risks arising from the digitalization process in different sectors, where technological innovation is integrated into the dynamics of care relationships, that are requiring new balances respect to the physical dimension.[8] This is both to meet the obligations set by regulations addressed to specific sectors and to align with the informative principles in the field, which are themselves enriched with new interpretative content for the necessary adaptations to maintain the effectiveness of the liability paradigm also in the digital dimension.

To this end, two positions are explored in this paper: children, who are vulnerable because of their legal incapacity unless represented, and patients, who are vulnerable due to their limited psycho-physical integrity. Before the digital dimension, in fact, they both become users (and potential consumers), adding a new ground of vulnerability due to the contractual asymmetry with the market players.

---

5 M. E. Kaminski, G. Malgieri, *Algorithmic impact assessments under the GDPR: producing multi-layered explanations*, in *International Data Privacy Law*, 2021, 125 <https://doi.org/10.1093/idpl/ipaa020>.

6 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

7 A. Gullo, *Il Digital Services Act e il contrasto alla disinformazione: responsabilità dei provider, obblighi di compliance e modelli di enforcement*, MediaLaws, 2023, 2, <https://www.medialaws.eu/rivista/sezione-monografica-il-digital-services-act-e-il-contrasto-alla-disinformazione-responsabilita-dei-provider-obblighi-di-compliance-e-modelli-di-enforcement-contenuti-scopi-e-traiettoria-della/>.

8 J.A. Sanchez, P. Barach, J.K. Johnson, J.P. Jacobs (eds), *Improving Safety, Quality, and Value*, Springer, 2017.

As a result, common principles are identified and their interplay with technical standards explored in order to achieve a common core of harmonised best practices that could help the *by design* protection of vulnerable groups in the digital dimension.

B. Risks and opportunities for children

The digitalisation of services and products impacted on the growth of children since the earliest stages of their lives[9]: new risks, but also new opportunities, addressed in the cyberspace require tailored approaches towards children's care and education.[10]

Global challenges launched for children and the ongoing initiatives aiming to shape an inclusive future generation of digitalized citizens are highlighting the increasing opportunities of access to culture and education offered by the information society, fostering the need to address fresh forms of free expression, organization, and association[11]. In the cyberspace, ideas and content are disseminated more rapidly and effectively. Furthermore, physical and mental well-being could be enhanced by empowering individual attitudes and skills through tailored paths of learning, experiencing, and playing in the digital dimension. Inclusivity can be promoted by providing broader chances to exchange experiences, knowledge, and values among the world being just connected to internet[12]. In this context, the acquisition of digital skills becomes imperative for the education of children. This is an especially delicate matter, given that UNICEF reports that nearly 65 million young people, approximately 90% of adolescent girls and young women aged between 15-23 years old remain without internet access[13]. Hence,

9 S. Livingstone, G. Lansdown, and A. Third, *The case for a UNCRC general comment on children's rights and digital media*, 2017, LSE Consulting/Children's Commission.

10 E. Marrus and P. Laufer-Ukels, *Global Reflections on Children's Rights and the Law 30 Years After the Convention on the Rights of the Child* (Routledge 2021).

11 See the OHCHR, *Children's rights and the 2030 Agenda for Sustainable Development*, https://www.ohchr.org/en/children/childrens-rights-and-2030-agenda-sustainable-development.

12 Committee on the Rights of the Child 'General comment No. 25 (2021) on children's rights in relation to the digital environment' (2021). <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en>.

13 The statistics refers to low-income countries, where almost 78% of young men and male adolescents are offline too (57 million persons), UNICEF, Bridging the Gender Digital Divide, Report, 2023, <https://data.unicef.org/resources/ictgenderdivide/>.

the digital divide among young generations concerns as it exacerbates the economic disparities, and it pertains to the cultural shifts affecting the daily routines of every child and their caregivers. The implementation of appropriate measures to ensure inclusivity, non-discrimination, and safety within the IoT shall thus be designed and applied as a standard to be followed in order to avoid the development of harmful mechanisms of access and use of digital services.[14]

The above-illustrated premises need to be balanced considering the different phases of growth and maturity of the given child, rather than solely relying on the formal definition of a minor. According to Article 1 of the UN Convention on the Rights of the Child (hereinafter CRC), adopted in New York in 1989, a minor is defined as "*every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier*". Despite this, in fact, one-third of the IoT users are aged between 11 and 16. Therefore, critical profiles arising from their daily engagement within information society services shall be not only addressed but also solved since risks might daily occur, becoming urgent harms for children's wellbeing[15]. In this regard, the GDPR is the first EU legislative initiative on data relying with children as a specific category of (vulnerable) data subjects. It established that consent to process data by information society services could be autonomously provided at 16 years old, leaving the Members States to identify a lower threshold up to 13 years old, considering that in the data protection impact assessment, the data controller would have addressed the vulnerability of children-users as a ground of specific analysis.

From this perspective, the fact that the new service launched by OpenAI Ldt, the well-known ChatGPT[16], has been limited by the Italian data protection authority because of the lack of safeguards to identify the age of potential users, stresses a lack of an attentive strategy, looking at the possible vulnerable categories of users in the digital environment, as well as the necessity to implement stricter obligations for services providers to

14 Ibid.

15 M. Boomgaard, *Children's Rights in Data Protection: A Comparative Analysis on Ex-Ante and Ex-Post Protection of Children's Data in the EU and the USA* (College of Europe 2016).

16 D. Amram, *Accountability, Transparency, and Fairness to Assess Generative AI Solutions with the Lenses of Data Protection Law*, Diritti Comparati, 2023 <https://www.diritticomparati.it/accountability-transparency-and-fairness-to-assess-generative-ai-solutions-with-the-lenses-of-data-protection-law/>.

specifically develop risks assessment procedures to protect such a vulnerable users category *by design* and *by default*.

While the so called AI Act just refers to children as vulnerable groups in *recitals* 16, 19 and 28, and in articles 5, sub d. i) and article 9 *sub* 8) stating that the risk assessment shall take into "*specific consideration (…) whether the high-risk AI system is likely to be accessed by or have an impact on children*", without providing any instrument to address it, the DSA covers this gap in article 35 *sub* j) where it presents a short list of organisational and technical safeguards, like "*age verification and parental control tools, reporting tools aimed at helping minors signal abuse or obtain support*". The DSA commitment to protect children is expressed also in the recital 71, stating that due-diligence obligations shall be applied to an online platform that can be "*considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors*", for example through personal data processing. In these cases, therefore, "*appropriate and proportionate measures to protect minors*" shall be implemented, including the design online interfaces reaching "*the highest level of privacy, safety and security for minors by default where appropriate or adopting standards for protection of minors, or participating in codes of conduct for protecting minors*". The recital identifies also as best practices and available guidance the ones provided by the communication of the Commission on A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). In particular, it recommends introducing specific safeguards in case of profiling activities based on personal data processing, in compliance with the principle of data minimisation that shall prohibit the online platform "*to maintain, acquire or process more personal data than it already has in order to assess if the recipient of the service is a minor*".

In this regard, it seems that the protection of children as users of digital services is a technical matter, aiming to firstly verify the age of the user in order to enable or prohibit the exposure to contents, services, and products. However, these technical standards might not be sufficient to address the challenges of an inclusive and safer digital environment as additional measures – including organisational ones – might be required to face specific harms emerging even for services directly targeted to children.

I. Harms in the digital environment

The EU Commission identified six different harms that may occur to children while accessing IoT as users.[17] The first relates to fake news, which authors have identified as falling into six different concepts, including content manipulation, satire, and advertising.[18]

By its misleading nature, fake news can have a negative impact on the development of children's opinions, whose discerning capacity and maturity are still in evolution.[19] In this regard, the DSA expresses the commitment of the EU Commission to address this risk as a general attempt to users' fundamental rights protection and empowerment. In particular, DSA compliance activities include the obligation to publish annual reports on content moderation practices, the one to set users friendly complaints mechanisms to make content removed if illicit or in contrast with inclusiveness, non-discrimination or fundamental rights. Furthermore, Very Large Online Platforms shall formally assess risks also connected to the content manipulation in order to avoid misuses as disinformation spreading, especially in crisis cases.

The second risk concerns exposure to cyberbullying.[20] For the victim, this can be shaped as a series of behaviours including an innocuous attitude to perpetrate moral disengagement as well as harmful exposures to disturbing content. The latter is perceived as a third autonomous risk when it becomes a -so-called- digital challenge/game directly offered to young users. The well-known case of the *Blue Whale*, consisting of proposing a series of tasks to depressed teenagers for a period, increasing time after time the relative level of self-harm until inducing players to suicide, has been followed by other challenges like *Chroming*.[21] Article 6 CRC states that children have

17 European Commission, *EUKidsOnline survey*, IP/11/479. See previous remarks on the topic in the contribution: D. Amram, *Children (in the digital environment)*, in G. Comandé (ed), Elgar Encyclopedia of Law and Data Science, 2022, 64 ff.

18 E.C. Tandoc, Z.W. Lim and R. Ling, *Defining "fake news": A typology of scholarly definitions*, 2017, Digital Journalism, 6, 137ff.

19 Council of Europe, *Challenges to Children's Rights Today: What Do Children Think*? (2015), Ch. 8.

20 S.C. Vestergaard (ed.) *Encyclopedia of Bullying* (Nova 2020).

21 F. Liat and G. Khalid, *The criminalization of cyberbullying among children and youth*, 2019, 17 Santa Clara J Int'l L 1ff. See the recent urgent measures adopted by the Italian Data Protection Authority against the Tik Tok platform following a 10-year-old child's death from an online challenge, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524224>; (2019); in May 2020 the Dutch DPA started an

an inherent right to life and, therefore, also within the digital environment they shall be protected from violence and suicide.[22] Such a protection may be compromised even in a technically robust system. Parents' awareness and collaboration with schools become essential to prevent harms for the given child, however at any level, each stakeholder shall contribute to avoid the described phenomena. In this regard, the well-known TikTok platform has been recently sanctioned by the European Data Protection Board for a dossier issued by the Irish data protection authority, because of the illicit data processing activities of underaged users[23].

Furthermore, children can be exposed to grooming and sexting both as users of social networks, platforms, etc., and where someone else shares their pictures, images, videos. To this end, national legal systems are implementing new provisions in order to address the digital dimension of these crimes.

As the digital dimension is based on data processing, it is not surprising that the data protection authorities are those ones that have more sanctioned services providers for exposing children to known risks of the Internet of Things. In fact, all the mitigation measures concern data processing activities. This is true also in case of AI-based solutions, where data processing is undertaken through an automated decision-making system. For example, in case of toys that can monitor and record children's habits, behaviours, voices, without their parents or adults or caregivers having any control over that kind of data processing or means and purposes of processing activities deployed after the data collection, two different risks might be envisaged: firstly, the *boomerang* effect of being target both for specific advertisement and manipulative marketing strategies and, secondly, for even unpredictable uses, since none has the control on that kind of information and safeguards that are applied to the data flows before being shared to third parties.[24] Further vulnerabilities might also be exposed

investigation into the same platform <https://autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-investigate-tiktok>.

22 Doek, J.E., *Article 6 CRC and the views of the CRC Committee*, 2015, 26 Stellenbosch L. Rev. 254.

23 EDPB, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), <https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en>.

24 B. Knowles, S. Beck, J. Finney, J. Devine and J. Lindley, *A scenario-based methodology for exploring risks: Children and programmable IoT*, DIS'19 Proceedings (2019) 751 ff.

through the combination of IoT services and AI-based technologies. For example, the increasing use of chatbot systems at home can increasingly affect teenagers' behaviours, becoming a kind of personal assistant to be checked for confirmation on possible outfit, or other daily attitudes that are shaping one's personal identity. [25]

Some of the mentioned risks could be mitigated by technical and organizational measures implemented by services providers and developers, especially if standards and codes of conducts are adopted. However, an essential role is played by adults (family members, teachers, educators, and professionals) that shall develop a digital education and be able to transmit competence and skills to detect and avoid dangerous circumstances.[26] A strong information and awareness campaign promoted by institutions (schools, social services, municipalities, etc.) has become a priority. A long-term commitment towards a cultural change shall be addressed to protect children as *per se* vulnerable users.

To this end, international organisations, like UNICEF, have produced tailored strategies aimed at promoting children's rights in the digital environment as a priority[27]. Other ones are developing specific studies to address these issues, for example the Joint Research Centre of the EU Commission has published a report in order to address future policies for a more ethical approach of AI-based systems for children: some applications have been mapped and classified in terms of risks and opportunities under a series of parameters, including accessibility, engagement for learning, adaptation, social interaction, health, transparency, inclusivity etc[28].

Considering the principles stated in the CRC, to protect children's rights in the digital environment means to develop a setting where they can enhance their freedoms to shape and express their opinion both as individuals and as belonging to groups, and at the same time not being

25 H. Alexa, S. Cortesi, A. Lombana-Bermudez and U.Gasser, *Youth and Artificial Intelligence: Where We Stand*, 2019, Berkman Klein Center for Internet & Society publication.

26 T. Leibur, L. Saks, I.A. Chounta, *Towards Acquiring Teachers' Professional Qualification Based on Professional Standards: Perceptions, Expectations and Needs on the Application Process*, 2021, Education Sciences, 11(8), 391 and I. Tuomi, R. Cachia, D. Villar-Onrubia, *On the Futures of Technology in Education: Emerging Trends and Policy Implications*, JRC Publication, 2023, <file:///C:/Users/denis/Downloads/JRC134308_01.pdf>.

27 UNICEF, *Policy guidance on AI for children*, 2020.

28 JRC, *Artificial Intelligence and the Rights of the Child*, 2022.

exposed to potential harms. Thus, the general principle of the best interests of the child stated under Article 3 CRC requires a specific balance in the digital dimension between rights and situations aimed at identifying case by case which conditions could satisfy the child's well-being.[29] Other principles, like the one of non-discrimination – stated by Article 2 CRC-, become paramount also within the EU regulations to establish a safer digital environment where equal access is guaranteed, despite of the existing digital divide between countries facilities. Socio-geographical-economic conditions shall not affect the possibility to enjoy fundamental rights in the digital dimension.[30] However, the exclusion from online services is an index of contemporary poverty and it is largely impacting on raising the new generation of adults. Therefore, for the most marginalized groups of children proper actions should be implemented to remove these barriers. In particular, it highlights the role of learning initiatives for children as a means to successfully avoiding the risks and exploiting the opportunities offered by the information society.[31] The COVID-19 pandemic emergency has highlighted this aspect, as everywhere – especially primary and secondary – schools moved to e-learning activities: the access to internet facilities was the means to allow children to remotely attend classes and keep pursuing their educational path. Moreover, access should not be denied, and content should be reliable and not harmful under the well-known grounds of inclusiveness assessment based on race, ethnic origins, political opinions, religious/philosophical beliefs, trade union memberships or sexual orientation. Conversely, a digital environment that could admit grounds of discrimination shall be completely prohibited and limited. Further challenges might be launched for the use of generative AI applications.[32]

Under Articles 12 and 13 CRC, children's right to be heard and the right to freedom of expression are promoted in IoT services.[33] In particular, Article 12 enhances participation in decision-making, while Article 13 includes

29 J. Todres and S.M. King, *The Oxford Handbook of Children's Rights Law* (OUP 2021); J. Tobin, *The UN Convention on the Rights of the Child: A Commentary* (OUP 2019).

30 T. O'Neill and D. Zinga, *Children's Rights: Multidisciplinary Approaches to Participation and Protection* (University of Toronto Press 2008).

31 Council of Europe, *Strategy for the Rights of the Child*, 2016–21, <https://edoc.coe.int/en/module/ec_addformat/download?cle=2d45cbe914655ca562553cb81fdfc464&k=43516ccd18e8b8e8d5d68b6fd3b7e4c1>.

32 UNICEF, *Generative AI: Risks and Opportunities for Children* (2023), <https://www.unicef.org/globalinsight/media/3061/file>.

33 S. Lee, *A child's voice VS. A parent's control: Resolving tension between the Convention on the Rights of the Child*, U.S. LAW' (2017) 117(3) Columbia Law Review, 687–727.

"*the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice*".

These rights could be empowered at different levels according to the maturity of the child. However, everyday online educational, training, or ludic activities mark the IoT as a place to develop individual and collective thoughts and opinions. Further, as illustrated, if we combine these principles with the exposure of the child to the manipulation of information and fake news, state parties should identify proper actions in order not only to guarantee the right to freedom of expression in the information society services but to enhance it towards inclusiveness and pluralism as an opportunity for children to grow in a child-friendly and safe environment. In this regard, the role of the EU Regulation on DSA is particularly relevant as well, where it states that manipulative techniques for advertisements are forbidden. The recital 69 of DSA explains, indeed, that advertisements based on profiling activities, using special categories of personal data are prohibited because they may "*amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups*".

II. Policies, guidelines, and standards

An equal access to a safe and fair digital environment and technologies application requires to address risks and detect mitigation measures. However, this is not sufficient, as institutions, public and private organisations, companies, and individuals shall responsibly contribute to grow up the next generation of adults as well.

According to article 19 CRC, for example, State Parties must adopt all legislative, administrative, social and educational measures to avoid any forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse. As we have seen, this principle is particularly sensitive in the digital age, considering the urgency to prevent the above illustrated phenomena like cyberbullying, grooming, sexting, primarily affecting child users. To introduce only control and monitoring systems cannot be the solution, since there is another general principle to be balanced: under Article 16 CRC, there is a prohibition on arbitrary or unlawful interference with children's privacy, family,

home or correspondence, which translates into a child-centred perspective the debate on privacy preserving and data protection in the digital age, also recalling the more recent formula included in Article 8 of the European Charter of Fundamental Rights.[34] Caregivers' and parental responsibilities become therefore the boundaries within which the child's autonomy may be framed in a sophisticated balance of rights and duties aimed at enhancing individual skills, while protecting them from risks and harms.[35]

The Council of Europe firstly adopted a Recommendation, namely the CM/Rec(2018)7 of the Committee of Ministers to Member States, providing guidelines to respect, protect and fulfil the rights of the child in the digital environment. This soft law mechanism aimed at driving the law and policy making processes in each State Party through the interpretation enshrined in human rights conventions as well as at including standards, emerging from relevant case law issued by the European Court of Human Rights.[36] Then, it launched a Strategy on the rights of Child 2022-2027, including safeguards addressed to the digitalisation and use of AI. The Guidelines appeared very useful to define the digital environment as the "*information and communication technologies (ICTs), including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services*". This allowed to foster safeguards implementations by services providers, parents, and caregivers, and all relevant stakeholders, all responsible to guarantee a safe and resilient setting. Guidelines addressed also the opportunity to engage children more effectively in the decision-making process by highlighting educational paths, skills, and best practices to increase the value of child-friendly technologies. To achieve the first goal, State Parties must ensure high standards of online services and contents. The Guidelines identified also the so-called "*distinctive opportunities*" to enable online communication, gaming, networking and entertainment with children both in play and to peaceful assembly and association. The Strategy fosters six objectives, aligned with the above-mentioned risks, including

34 M. Ruiz-Casarez, T.M. Collins, E.K.M. Tisdall and S. Grover, *Children's rights to participation and protection in international development and humanitarian interventions: Nurturing a dialogue*, International Journal of Human Rights, 21, 2018 doi: <https://doi.org/10.1080/13642987.2016.1262520>.

35 B. Shmueli and A. Blecher-Prigat, *Privacy for children*, Columbia Human Rights Law Review, 42, 2011, 759 ff.

36 S. Livingstone, E. Lievens and J. Carr, *Handbook for Policy Makers on the Rights of the Child in the Digital Environment* (2020) COE <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>.

to keep children safe from violence, to guarantee equal opportunities in the current society, to support access to new technologies, to give them voice and participation, to support them in emergency situations and crisis, and develop a child-friendly justice. The main current challenge is to promote these objectives either in the physical dimension or in the digital one.

As far as child's best interests are concerned[37], the first condition for a child-friendly data-driven economy is to identify the proper methodological approaches to combine compliance *by design* and tailored decision-making in the given circumstances for each specific digital service/tool/activity/product. This approach should be adaptable according to a series of variables that may include, as seen, age and maturity of the user, digital skills both of the child and her parent/caregiver, exposure to each of the mentioned risks, level of awareness, etc. It should also include monitoring mechanisms to report gaps and detect best practices in order to achieve an everyday higher level of trustworthiness.[38] In fact, decision-making or data processing that could be acceptable for adults may not be so for children and, therefore, appropriate technical and organizational measures should be implemented to guarantee conformity with CRC principles in the digital dimension.

Current debates on AI, robotics, and digital services[39] regulations are not addressing specific technical and organizational measures for a child-friendly paradigm to comply with *by design* and *by default*. In particular, policy and law-making efforts are driven towards common requirements and standards for developers, intermediaries, service providers, etc. without highlighting the vulnerabilities emerging where children are the data subjects/end users. Thus, the role of parents, caregivers, educators, facilitators are the main driver to ensure case by case the pursuing of the best interests of the child in the use of AI-based technologies/digital services. As observed, this approach is not sufficient to empower children's rights if we consider the peculiarity of risks and opportunities that solutions from

37 E. Lamarque, *Il principio dei best interests of the child nella prospettiva costituzionale* (Franco Angeli 2016).

38 High-Level Expert Group on AI (2020) 'Ethics guidelines for trustworthy artificial intelligence', <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

39 Proposal for a regulation on a European approach for artificial intelligence, in <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence>.

research and innovation development are bringing to children's everyday life.

In this regard, UNICEF proposed to fill such a gap, by drafting the Policy Guidance on AI for Children.[40] It identified nine requirements for child-centred AI, including recommendations on how AI techniques could be made suitable for children's well-being and safety, as well as to prepare them for future technological developments. These recommendations, however, require to be associated with technical requirements in order to find concrete applications in the services and products offered to children as users of the new technologies.

In this regard, standards developed by the Institute of Electrical and Electronics Engineers, namely the IEEE 2089-2021, are supporting the development of tailored procedures aiming to encompass the following key principles: the fact that the given system shall recognise if the user is a child; the fact that it is mandatory to distinguish children from young people as different categories of users; the fact that interfaces shall use of child-friendly language; the fact that within the balance between commercial interests and children's ones the latter shall prevail[41].

In this debate, the GDPR plays a pioneering role for two reasons. Firstly, it constitutes an example to protect personal data by including a risk-based data subjects-oriented approach aimed at continuously assessing the impact of each component of data processing (i.e. the means, purposes, nature of data, subjects, technology adopted). Secondly, Article 8 GDPR is dedicated to minors' consent for online data processing, opening new interpretations on the balance between the formal legal age and the actual maturity of young users. [42]

40 UNICEF, *Policy guidance on AI for children*, n. 27 above.

41 IEEE, *IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*, 2021, <https://standards.ieee.org/ieee/2089/7633/>.

42 As mentioned, the framework becomes more complex as the same provision that states that a 16-year-old child can give valid consent for IoT data processing, it also leaves the opportunity for member states to decrease the age limit to 13 years. This last limit is the same as that introduced in the US Children Online Privacy Protection Act (COPPA), effective since 2000.L.A. Matecki, *Update: COPPA is ineffective legislation! Next steps for protecting youth privacy rights in the social networking era*, 2010, 5 Nw. J. L. & Soc. Pol'y. 369 http://scholarlycommons.law.northwestern.edu/njlsp/vol5/iss2/7, during the publication of this essay, new protections have been enacted for teens though the Kids Online Safety Council (KOSA) and the COPPA 2.0 bills, see S.1409 — 118th Congress (2023-2024), <https://www.congress.gov/bill/118th-congress/senate-bill/1409/text>.

In light of these remarks, a second challenge for child-friendly data economy consists of considering the digital dimension as a new scenario where children's rights must be protected, promoted, and enforced. Therefore, a multilevel paradigm towards parental responsibilities[43] must be adopted in order to include tailored actions and proactive approaches to child-friendly innovation and technologies.

In particular, proper roles and responsibilities have to be identified for parents/caregivers/facilitators in order to develop digital skills and competence and at the same time develop a privacy-preserving awareness to avoid digital-related risks.[44] An accountable approach would thus be adopted since the development of the given service/product addressed to children. It shall be indeed pursued by adults in a continuing balance of new knowledge and skills development functional to monitoring and detecting new harms and risks in order to prevent them[45].

More generally, parents and caregivers should thereby ensure education, care, and maintenance duties also in the digital environment, highlighting the different roles of each adult in a multilevel system of obligations and duties that might align with the concepts of responsibility, accountability, and liability in the digital dimension.

Finally, a child-friendly setting should be developed through proper actions and safeguards to address further vulnerabilities of children to concretely contribute to the purposes of inclusiveness and non-discrimination. For example, disabilities, socio-economic barriers, education gaps, digital divide issues are particularly sensitive ones for children as they may dramatically affect their growth and development in society. Specific attention shall therefore be addressed to vulnerabilities within the "children" as a category of users. For example, children with disabilities may constitute a specific category of vulnerable users. Risks and opportunities shall be addressed also in light of the specific principles stated for disabled persons, like for instance in the context of the Convention on the Rights of Persons

43 D. Amram, In familia respondēre. *La famiglia alla prova della solidarietà e del principio di responsabilizzazione. Contributo ad una ricostruzione sistematica* (Torino, 2020) 1–252.

44 J. Albo-Canals, D. Amram, K. Kaesling, J. Martinez Otero, R.G. Pensa et al., *Children's rights in online environments with social robots: The use case study of CORP: A collaborative online robotics platform'*, ACM, 2021.

45 See also A. Pera – S. Rigazio, *Let the children play. Smart toys and child vulnerability*, Chapter 14.

with Disabilities.[46] Disabled children's quality of life, indeed, might be strongly improved by the digitalisation of services and products and the digital transition of healthcare, education, and more general of economy. Thus, the information society services could be considered as a bridge for inclusiveness in certain circumstances, but only when it is safe and reliable for multiple level of vulnerabilities of the users' categories.[47]

To better address vulnerabilities emerging from the compromission of the psycho-physical integrity, it is worth to explore how the digitalisation is impacting on the patient-clinician relationship.

C. Patients and clinicians

In this paragraph, we explore the effects of the digital transition of the healthcare services in order to address and mitigate the emerging vulnerabilities respect to the two main categories of stakeholders: the patients and the clinicians.

As known, the digitalization of healthcare services can encompass both diagnostic and treatment phases, activating patient participation in the process of personalized care. This is often referred to the so-called *P5 Medicine*, indicating technologies that promote i) predictive, ii) preventive, iii) personalized, iv) participatory, and v) psycho-cognitive medicine through the application of digital and AI-based technologies, arising ethical and legal issues to be addressed in order to mitigate new (and old) vulnerabilities for an effective improvement of the healthcare system.[48]

As a self-evident method to detect vulnerabilities we will address the concept of "sensitive" information represented by the notion of data belonging to specific categories under Article 4 GDPR[49]. Sensitive, as stated, is the

46 M. Alper and G. Gogging, 'Digital technology and rights in the lives of children with disabilities' (2017) New Media & Soc., 19(5): 726–40.

47 L. Lundy, B. Byrne, M. Templeton, and G. Lansdown, 'Report on children with disabilities in the digital environment' (2019) <https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f>.

48 See in D. Amram, A. Cignoni, T. Banfi, G. Ciuti, *From P4 medicine to P5 medicine: transitional times for a more human-centric approach to AI-based tools for hospitals of tomorrow*, Open Research Europe, 2022, 2:33 <https://doi.org/10.12688/openreseurope.14524.1>.

49 G. Comandé, G. Schneider, *Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of 'Health Data'*, in European J. Health Law, 2018, 284 ff. <https://dx.doi.org/10.1163/15718093-12520368>. G. Bincoletto – P. Guarda,

information that can reveal certain characteristics of the data subjects and, for this reason, make them vulnerable in relation to their peer group. Information related to one's health status, for example, classifies the individual as a patient rather than a healthy person, profiling a potential vulnerability in their physical or mental sphere: therefore, health-related information produces a declarative effect of the vulnerability.

In this regard, the passage from the physical to the digital dimension, nothing changes for the identification of patients as a category of vulnerable persons.

The digitalization of the processing activities of health-related data, namely collection, use (and reuse), indeed, may have increased the risk of compromising the confidentiality of information included in data flows (through the increasement of occurrence that unauthorized access or unauthorised further processing might be performed, for example), but at the same time, it reduced the likelihood of information unavailability (primarily due to possible backup copies included in any data breach policy), contributing to a more effective management of the informative flow[50]. The same effect occurs with regard to the integrity of information: compared to paper-based support, the traceability of actions required to manage health-related data in the digital environment reduced the consequences of human errors, by allowing effective and faster countermeasures for content restoration/correction.[51]

An efficient data management may therefore facilitate the provision of healthcare services, but it may arise some issues within the clinician-patient relationship in terms of impact of the digitalisation on the asymmetry information between "professional" and "customer" roles. Therefore, it

A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data, Opinio Juris in Comparatione, 2021, 43 ff.

50 ENISA, *Data Pseudonymisation: Advanced Techniques and Use Cases*, 2021 <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>.

51 G. Wang, A. Badal, X. Jia et al., *Development of metaverse for intelligent healthcare*, in *Nat Mach Intell*, 2022, 4, 922 <https://doi.org/10.1038/s42256-022-00549-6>. Si veda G. Lofaro, *Dati sanitari e e-Health europea: tra trattamento dei dati personali e decisione amministrativa algoritmica*, in *MediaLaws*, 2022, 3, <https://www.medialaws.eu/rivista/dati-sanitari-e-e-health-europea-tra-trattamento-dei-dati-personali-e-decisione-amministrativa-algoritmica/>.

is extremely relevant to assess if and how the vulnerability may change through the digitalisation of the patient-clinician alliance.[52]

Firstly, the use of new technologies introduces an "intermediation" into the clinician-patient relationship, namely the human-machine interface that requires a tailored interaction, for instance, this is particularly evident in the case of robotic surgery, where healthcare services provision is mechanically supported by a tool solely driven by the surgeon. Secondly, while depersonalizing certain aspects of healthcare services, especially those related to data processing from analysis, technology enables greater personalization of other aspects of the same ones. By comparing a specific clinical framework with vast amounts of similar scenarios, there is an evident potential for improving the accuracy of the diagnosis and a simultaneous reduction in the overall state of vulnerability, meant as the compromission of psychophysical integrity of the patient. In this context, the clinician-patient relationship is supplemented by the human-machine component[53], which needs to be addressed both in terms of the relationship between the digital element and healthcare staff and with respect to the patients (and their vulnerabilities).

To investigate the impact on fundamental human rights and, consequently, assess the risks for their violation, it is observed that, in relation to healthcare staff, technological support must be accompanied by specific training aimed at developing skills for monitoring and intervening in the event of malfunction or inadequacy of the machine for the specific task. Additionally, healthcare professionals should acquire new interpretative methodologies for the results of automated processes to support decision-making operations in diagnosis or treatment.[54] From the patient's perspective, a series of issues arises regarding the need to ensure self-deter-

52 The Economist, *A digital revolution in health care is speeding up*, 04.03.2017; H.S. Sætra, E. Fosch-Villaronga, *Healthcare Digitalisation and the Changing Nature of Work and Society*. Healthcare (Basel). 2021 Aug 6;9(8):1007. doi: 10.3390/healthcare9081007.

53 D. Larrivee, *Values Evolution in Human Machine Relations: Grounding Computationalism and Neural Dynamics in a Physical a Priorism of Nature*, in *Front. Hum. Neurosci*., 2021, 15:649544. doi: 10.3389/fnhum.2021.649544.

54 L. Lessard, W. Michalowski, M. Fung-Kee-Fung, L. Jones and A. Grudniewicz, *Architectural Frameworks: Defining the Structures for Implementing Learning Health Systems*, in *Implementation Science* 12(1) (2017) 78. DOI: 10.1186/s13012-017-0607-7.

mination[55] in healthcare choices in the digital dimension and beyond.[56] There are multiple ethical and legal aspects to addres[57]: from the conditions for achieving a satisfied level of trustworthiness in the performance of machines supporting clinical services, to mechanisms to share awareness on the consequences of data collection for potential reuse, to the need to train the system to improve the accuracy of services for altruistic purposes, including research, experimentation, statistical analysis for the overall advancement of diagnostic, treatment, and rehabilitation capabilities. Given that the result of the balance between the risks and opportunities of digitalization in the relevant sector should ideally yield a positive value, it is necessary to categorize vulnerabilities in a variety of scenarios in order to be able to shape a unified methodology to provide policy guidelines for a virtuous acceleration of the introduction and use of digital systems in healthcare facilities.[58]

Firstly, we may distinguish the state of emergency, from routine circumstances, like outpatient screening or surgical procedures, where standards and protocols are regularly applied with no exception like in the emergencies. Additionally, we need to address the increasingly common situation where patients actively participate in care and rehabilitation activities through monitoring devices and dedicated apps, where the active and informed role of the vulnerable subject is an essential part of the strategy effectiveness of the telemedicine services. [59]

I. Vulnerabilities in digitalised emergency, outpatient, and surgical services

Within the emergency scenario, for example, the digitalization of first aid operations represents a significant opportunity for operative coordination

55 G. Resta, *La regolazione digitale nell'Unione Europea. Pubblico, privato, collettivo nel sistema europeo del governo dei dati*, in *Riv. Trim. Dir. Pubb.,* 2022, 971 ff.

56 L. Palazzani, *Informed consent for clinical research in the context of the Covid-19 pandemic between bioethics and biolaw: a general overview*, *BioLaw J*. <https://doi.org/10.15168/2284-4503-843>.

57 M.H. Arnold, *Teasing out Artificial Intelligence in Medicine: An Ethical Critique of Artificial Intelligence and Machine Learning in Medicine*, in *Bioethical Inquiry* 18, 121–139 (2021) <https://doi.org/10.1007/s11673-020-10080-1>.

58 J. Pizoń, A. Gola, *Human–Machine Relationship—Perspective and Future Roadmap for Industry 5.0 Solutions*, in *Machines*, 2023, 11, 203 <https://doi.org/10.3390/machines11020203>.

59 See previous remarks in D. Amram, *La transizione digitale delle vulnerabilità e il sistema della responsabilità*, in *Riv. It. Med. Legale,* 2023, 1 ff.

through personal (and non-personal) data sharing. This approach requires the identification of a proper legal basis justifying such processing activities. In fact, the extraordinary and temporary situation in which natural or artificial events disrupt the normal sequence of actions and events as well as the direct or indirect involvement of persons in an emergency situation constitute *per se* a case of vulnerability. Indeed, physical and mental well-being - as well as the emotional, economic, social, or environmental conditions - can be differently affected by dealing with a specific emergency situation.

Data-driven technologies may process personal data under a series of conditions that may satisfy the lawfulness both under Article 9(2)(c), the vital interests of the data subject or third parties when "*the data subject is physically or legally incapable of giving consent*", and under Article 9(2)(i), public interest in the field of public health. In these cases, it is relevant to define where the data processing begins (through direct or indirect collection of information) and where it ends. In particular, to enable possible further processing (the so-called reuse of collected information), especially after the emergency situation, tailored technical and organizational measures must be implemented to the same data flow, also addressing different legal bases.[60] For example, measures such as the pseudonymization and encryption of data to remain within the bounds of lawfulness of processing might be required to switch from the emergency legal basis to the one enabling the reuse for statistics and research purposes, under for example Article 89 GDPR. These conditions are the same either in case of paper-based or digital informative flows. More complex is the question related to the governance of data flows if they are digitalised and if the converges in an everyday more frequent digital platform aiming to collect data, combining the different sources of triage services (from the ones collected *in situ* by first responders to those collected through geo-localisation systems, *eg* drones and other systems). It seems reasonable to consider that data collected to face emergencies could be processed by public organizations, as well as by private or public ones engaged in activities related to the

60 L. L. Skovgaard, S. Wadmann, K. Hoeyer, *A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good*, Health Policy, Volume 123, Issue 6, 2019, 564 ff. <https://doi.org/10.1016/j.healthpol.2019.03.012>. See also the special issue G. Malgieri – P. De Hert, *Legal and Ethical Challenges of Data Processing in the research field*, in *Computer Law & Sec. Review*, 2020, 37 <https://www.sciencedirect.com/journal/computer-law-and-security-review/special-issue/10S60T5Q4Z8>.

described purposes. The development of technologies associated with systems aiming to develop unique triage sessions must take into account a series of regulatory aspects to prevent vulnerable individuals from being exposed to risks not mitigated by appropriate technical and organizational measures. In particular, the system must strive to comply with the principles of lawfulness, proportionality, minimization, and accountability, even in situations involving different jurisdictions. It should proactively identify which data shall be enabled or denied, for how long, and to which systems, both for incoming and outgoing data flows. It will also be necessary to identify countermeasures in the event of malfunctions to ensure the ability to restore the state of affairs in case of unauthorized loss, access, or modification as quickly as possible, so as not to compromise rescue operations. To this end, technical and procedural standards play an essential harmonising role at national, EU, and transnational level.[61]

Once the emergency management phase is completed, it is necessary to understand if (and how) the collected information can be reused for additional and different purposes. This perception may change from the physical to the digital collection of information. In fact, all possible players of first response activities might have interest to reuse the collected data for other purposes than the ones that enabled the original processing. For example, needs related to the evaluation and organization of first aid services may allow local (and non-local) oversight bodies to extract aggregated information to understand the scope of the intervention. However, it is necessary to define boundaries opening a generated database. From this perspective, anonymized data collected for public healthcare and similar purposes reasonably fall within the scope of the Open Data Directive and the Regulation on European data governance, also known as the Data Governance Act.[62] Unless there are reasons of public security, no limits appear to be set to making the collected data freely available in an intelligible format. Regarding personal data, especially health related ones, the natural

61 S. López Bernal, M. Quiles Pérez, E. T. Martínez Beltrán, M. Martín Curto, Y. Yanakiev, M. Gil Pérez, G. Martínez Pérez, *Opportunities for standardization in emergency scenarios in the European Union*, International Journal of Medical Informatics, Volume 179, 2023, <https://doi.org/10.1016/j.ijmedinf.2023.105232>.

62 See G. Carovano, M. Finck, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, Computer Law & Security Review, Volume 50, 2023, 105830 <https://doi.org/10.1016/j.clsr.2023.105830>; D. Amram, *Comparing EU Initiatives on Data: Addressing Risks and Enhancing Harmonisation Opportunities*, in *Opinio Juris in Comparatione*, 2023, 1 ff. <https://www.opiniojurisincomparatione.org/wp-content/uploads/2023/03/Amram_Online-First-1.pdf>.

subsequent destination after the initial first aid appears to be a medical record for the individual's healthcare purposes, thereby falling within the scope of Article 9(2)(h) of the GDPR.

In routine healthcare services, particularly in the outpatient scenarios, the primary use of patient data is governed by the healthcare purpose. However, it is important to note that the classification of information related to the individual's health status and its comparison with similar cases are part of the clinical method, even before the experimental one. The reconstruction of the clinical framework, especially in screening programs, results in data collection that needs to be classified and processed for decision-making purposes. The support of digital technologies in these activities is becoming increasingly common and incorporated into outpatient protocols and procedures. However, such technologies should be communicated to the patient to obtain informed consent, taking into account the implications for the established trust relationship with the clinician.[63]

The so-called social contact[64] that characterizes the relationship between the clinician and the patient undergoes adaptations in case of technological support that deserve to be analysed and interpreted in the context of the evolution of the information society. In particular, two scenarios are identified. The technological support for outpatient activities could still be in the study phase and patients are recruited based on a specific protocol approved by the relevant ethics committee. From the patient's perspective, they can choose whether to participate in the experiment or not, and the decision not to use technological support for healthcare provision shall not affect the clinician-patient relationship. Consequently, the patient can choose whether or not to provide consent to the use and reuse of data collected for experimental purposes. In this case, the patient's vulnerability is determined not only by their health conditions, but also by the informative

63 M. Jungkunz, A. Köngeter, K. Mehlis, E.C. Winkler and C. Schickhardt, *Secondary Use of Clinical Data in Data-Gathering, Non-Interventional Research or Learning Activities: Definition, Types, and a Framework for Risk Assessment*, in *Journal of Medical Internet Research* 23(6) (2021) e26631, doi: 10.2196/26631.

64 F. Giardina, *Responsabilità contrattuale ed extracontrattuale: significato attuale di una distinzione tradizionale*, Milano, 1993, F.D. Busnelli, *Verso un possibile riavvicinamento tra responsabilità contrattuale ed extracontrattuale*, in *Resp. civ. prev.*, 1977, 784, Id., *Itinerari europei nella «terra di nessuno tra contratto e fatto illecito»: la responsabilità da informazioni inesatte*, in *Contr. e impr.*, 1991, 539 ff., R. Pardolesi - R. Simone, *Nuova responsabilità medica: il dito e la luna (contro i guasti da contatto sociale?)*, in *Foro it.*, V, 2017, 4, 167.

asymmetry related to the development of the given experimental protocol, which must include specific risks mitigation measures for the system used in the particular outpatient setting. Additionally, ethical and legal assessments are made regarding the reliability of the algorithmic system used to make automated decisions for diagnostic and treatment purposes as a part of the ethical protocol.[65] The second case concerns the technological support for outpatient activities that is already integrated into the regular protocol of the service. The information system is an essential part of the equipment necessary for service delivery, and the patient, adequately informed, may not find alternatives to the use of the given technology for the provision of the healthcare services in that facility. The refusal of consent would thus result the inability to provide the service. However, also in this case patients shall maintain the control upon their information, and they can always prevent the reuse of their data by denying the consent to that specific data processing.

When the two described scenarios are each other consecutive, it seems reasonable to consider opening a phase of organizational and professional adaptation for the healthcare personnel affected by the introduction of technological innovation into the system. In fact, in the event that the experimentation is successful, and the new device is authorized by the competent ministry to be marketed or introduced into the corresponding department, it is necessary to put oneself in the position of the clinician and delve into the critical issues that may arise regarding the provision of the service in the daily context. In other words, in order to reshape the standards of diligence in light of the innovative element, it will be necessary to undertake a series of initiatives aimed at mitigating the vulnerabilities arising from the human-machine relationship [66] and identifying possible additional issues that may arise in that specific environment.

---

65 N. Naik, B.M.Z. Hameed, D.K. Shetty, D. Swain, M. Shah, R. Paul, K. Aggarwal, S. Ibrahim, V. Patil, K. Smriti, S. Shetty, B.P. Rai, P. Chlosta and B.K. Somani, *Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?*, in *Front. Surg*., 2022, 9:862322. doi: 10.3389/fsurg.2022.862322.

66 See the High-Level Group on Trustworthy AI, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment, see K. Hawley, *How to Be Trustworthy*, Oxford Un. Preff., 2019. M. Agbese et al., *Governance in Ethical and Trustworthy AI Systems: Extension of the ECCOLA Method for AI Ethics Governance Using GARP*, 2023, E-informatica: Software Engineering Journal 17.1 e R.V. Zicari et al., *On Assessing Trustworthy AI in Healthcare: Machine Learning as a Supportive Tool to Recognize Cardiac Arrest in Emergency Calls*, in *Frontiers in Human Dynamics*, 2021, 3.

From this perspective, a new category of vulnerable persons emerges: the one of the healthcare staff that needs to develop specific professional skills and competence to deal with the new technology. In particular, it is essential that the training will be aimed to avoid possible distortions caused by excessive reliance on technological support[67], or conversely, reluctance driven by the fear of a machine's substitutive effect or the individual clinician's cultural and educational context. New roles might emerge in the organisation. In fact, specialized skills aimed at preventing malfunctions or safely activating functionality restoration plans in case of defaults should be associated with the development of intervention capabilities in a domain that is different from the healthcare one. The composition of the staff - and thus the work shifts - should also take into account, the greater or lesser predisposition to use the new tool to avoid negatively impacting the quality of delivered services.[68]

In addition to outpatient activities, new technologies are increasingly finding their place in surgery rooms. In fact, advances in the field of surgical robotics guarantee the execution of specific tasks with high standards of precision and accuracy through the supervision of the healthcare professional guiding the device. Thus, representations of virtual environments allow for the planning of increasingly complex procedures and anticipate, through simulation, the possible consequences of certain actions and choices in the virtual twin scenario, thereby increasing the level of accuracy of the procedure and significantly reducing the chances of error and, consequently, of harms for patients.

From the patient's perspective, in order to create the digital twin of the operating room setting, at least the recording and reproduction of vital conditions and parameters shall be expected as the data processing activity necessary to perform the surgery. Therefore, information systems must guarantee the availability, integrity, and confidentiality of data flows to prevent, for example, patient-related values from short-circuiting or being replicated on machines associated with other subjects, or to ensure interoperability of communications when the assembly with other tools is neces-

67 Committee on Social Affairs, Health and Sustainable Development, *Artificial intelligence in health care: medical, legal and ethical challenges ahead*, 2020 <http://www.assembly.coe.int/LifeRay/SOC/Pdf/TextesProvisoires/2020/20200922-HealthCareAI-EN.pdf>.

68 European Parliamentary Research Service, *Artificial intelligence in healthcare*, 2022 <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf>.

sary. The risks related to privacy protection must, therefore, be assessed, mitigated, and monitored not only at the time of the introduction of the digital twin system in the operating room, but also during individual procedures[69]. It is necessary, in fact, for a series of parameters to be continuously monitored to ensure the functionality of the system, so that reality becomes computable, communications more flexible, and processes optimized. In particular, the management of the virtual space must be robust and reliable, providing high standards of security in the authorization architecture for performing individual operations, as well as contractual clauses capable of allocating roles and responsibilities, while maintaining an appropriate level of confidentiality for the nature of the data being processed.[70]

Among the advantages of using such technologies, considering the position of the surgeon and their respective staff, ergonomic comfort during the operation stands out. This leads to better precision of movements, reducing the likelihood of tremors, and also facilitates access to anatomically challenging areas, thanks to the possibility of having a three-dimensional or augmented representation of the surgical site. However, a new digital vulnerability to be addressed concerns the gap between perception and reality in the virtual or augmented environment, which may be experienced differently by the operator depending on their physical and/or emotional conditions. Studies in this field emphasize the need to assess the reliability and validity of the system through tests that highlight the behaviours of the operators when interacting with virtual reality.[71] This helps identifying the suitability requirements for operators to safely use digital twin technology.

The benefits for the patient, indeed, are related to the accuracy and precision of the machine: generally, minimal incisions limit post-operative effects (such as pain, infections, etc.) and reduce recovery times, including

69 V. Damjanovic-Behrendt, *A Digital Twin-based Privacy Enhancement Mechanism for the Automotive Industry*, *in International Conference on Intelligent Systems (IS)*, Funchal, Portugal, 2018, 272-279, doi: 10.1109/IS.2018.8710526, Z. Chen, J. Wu, W. Gan and Z. Qi, *Metaverse Security and Privacy: An Overview*, *in IEEE International Conference on Big Data (Big Data)*, Osaka, Japan, 2022, 2950-2959, doi: 10.1109/BigData55660.2022.10021112.

70 C. Alcaraz - J. Lopez, *Digital Twin: A Comprehensive Survey of Security Threats*, in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, 1475-1503, third quarter, 2022, doi: 10.1109/COMST.2022.3171465.

71 D. R. Sanchez, E. Weiner, A. Van Zelderlend, *Virtual reality assessments (VRAs): Exploring the reliability and validity of evaluations in VR*, https://doi.org/10.1111/ijsa.12369; E. Weiner - D. R. Sanchez, *Cognitive ability in virtual reality: Validity evidence for VR game-based assessments* <https://doi.org/10.1111/ijsa.12295>.

hospitalization. Again, the role of technical standards is paramount to develop procedure able to fulfil ethical and legal requirements for a trustworthy use of digitalised healthcare services.[72] All of these remarks are true in an ideal scenario where the healthcare professional-machine relationship is well-established and accepted.

Another critical aspect that arises in the digitalisation of healthcare services is related to the reuse of collected information for screening purposes. As mentioned for the emergencies, also in these cases, it is necessary to identify the legal basis that can justify the reuse of data collected for healthcare purposes and design an effective governance for information access and sharing. These activities usually require the development of digital platforms and infrastructures capable to securely managing incoming and outgoing flows, identifying roles and responsibilities to comply with regulatory obligations, including the need for pseudonymization, allocation of access and sharing privileges, or performing activities.[73]

In this regard, the proposed regulation for a European Common Space for Health Data states that there must be a separation between those ones who generate the data, those who manage them, and those who request access for reuse. This is to ensure the anonymity of patients (data subjects) whose pseudonymized data, through subsequent processing, could potentially enable re-identification.

The mediation of the clinician-patient alliance through human-machine interfaces is particularly evident within telemedicine scenarios, where it is applied through remote communication for the collection of those parameters, which, if connected to mobile phone applications and/or wearable devices, may gather information, process it, and allow - with the clinician's validation - to provide prescriptions, dosages, instructions for the continuation of treatment or rehabilitation pathways, etc., in other words, to remotely deliver supporting healthcare services.[74] Boundaries on the nature

72 Wen Sun et al., An Introduction to Digital Twin Standards, GetMobile: Mobile Computing and Communications, Volume 26, Issue 3, September 2022,16–22 <https://doi.org/10.1145/3568113.3568119>.

73 J-S. Bergé - S. Grumbach - V. Zeno-Zencovich, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law & Governance*, 5, 2018, 144.

74 See the EU Commission Communication COM(2008)689; Italian Ministry of Health, *Telemedicina. Linee di indirizzo nazionale* <https://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf>; Istituto Superiore Sanità instructions, *Indicazioni ad interim per servizi assistenziali di telemedicina durante l'emergenza*

of the healthcare services, for example, have been included in tailored guidelines[75], like the Italian ones identifying technical and organisational safeguards to frame telemedicine: from the assessment on possible cultural, digital, environmental barriers for the patient by the clinician, to the certifications required to the adopted software.[76] In fact, access to a stable internet connection, proven interoperability of the healthcare software with the operating system installed on the patient's devices, the presence of system recovery mechanisms in case of power outages, confirmed presence of antivirus software to prevent unauthorized access, are just some of the elements to be considered for the activation of such telemedicine services. Furthermore, the effectiveness of technological innovation will be as efficient as the patient (or the caregiver) is able to correctly perform the procedures. Therefore, if the patient demonstrates the ability to wear the device properly, set up the collection and transmission of information following the provided instructions, and, last but not least, manage and understand digital communication to continue treatment.[77] The digital divide shall be considered as *a priori* obstacle to the prescription of telemedicine support, considering the appropriateness standards of care[78]. Within this framework, the role of the vulnerable subjects, namely the patients, can be enriched with new aspects that make them more involved, aware, and an active leading actors in their own care journey.

---

sanitaria COVID-19, 12/2020 <https://www.iff.it/documents/20126/0/Rapporto+ISS+COVID-19+n.+12_2020+telemedicina.pdf/387420ca-0b5d-ab65-b60d-9fa426d2b2c7?t=1587114370414>.

75 Italian Ministry Decree, 21.09.2022 recante *Approvazione delle linee guida per i servizi di telemedicina - Requisiti funzionali e livelli di servizio*.

76 A. Sorrentino; L. Fiorini; G. Mancioppi; F. Cavallo; A. Umbrico; A. Cesta; A. Orlandini, *Personalizing Care Through Robotic Assistance and Clinical Supervision*, in *Frontiers in Robotics and AI*, 2022 <https://www.frontiersin.org/articles/10.3389/frobt.2022.883814/full>.

77 From this concept we may shape the content of the principle of appropriateness in healthcare, see AA.VV., M. Sesta (ed.), *L'erogazione della prestazione medica tra diritto alla salute, principio di autodeterminazione e gestione ottimale delle risorse sanitarie*, Maggioli, 2014.

78 See G. Finocchiaro, *Intelligenza artificiale e responsabilità*, in *Contr. impr.*, 2020, 724; U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. dir. civile*, 2020, 1246 f.; A. Fusaro, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova Giur. Civ. Comm.*, 2020, I, 1344 ff.

D. The interplay of technical and organisational standards to protect users

In the previous paragraphs, we have outlined some critical issues that can arise in a variety of scenarios where the provision of digital services and products are addressed to vulnerable users, like children, and patients. We identified risks to be mitigated in relation to data flows capable of exposing persons to new vulnerabilities and assessed the critical issues for those individuals who are not normally considered as vulnerable – such as adults, parents, caregivers, and clinicians – when they become so in relation to technological innovation, for example, due to a lack of knowledge or awareness of specific risks related to the digital dimension of their activities or of the ones performed by vulnerable persons they are taking care of. We also analysed how the exposure to the risk of compromising fundamental rights increases for individuals who are already vulnerable – such as patients – for various reasons, such as the potential loss of control over the information concerning them that are more easily exploitable in the digital environment than in the physical one.[79]

Furthermore, we deepened the fact that despite the risks associated with the digitalization and innovation of services and products, the scope of opportunities is disruptive not only in the clinical and scientific fields – where advances in time and quality of diagnosis, treatment, and care are already proven – but also in terms of access to culture, inclusion and education as a societal revolution, looking especially at children, as the citizens of tomorrow. This result is confirmed where multiple vulnerabilities shall be overcome in the same context, like in case of disabled children care and education sector: the data-driven society may strongly improve their quality of life, making the difference in terms of personalised services and inclusion strategies.[80]

In the data economy, as illustrated, the reuse of information serves as an asset to boost innovation in every sector. The impact of the digital transition on services and products deals with a series of aspects, touching both digital vulnerabilities and the vulnerabilities in the digital environment. To this end, the development of technical standards may improve not only the performance – and therefore the quality- of services and products, but it may also increase the trustworthiness in terms of ethical and legal

79 J. Van De Hoven et al., *Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications*, in *Opinio Juris in Comparatione*, 2021, 131 ff.

80 UNICEF, *Global report on assistive technologies*, 2015 <https://www.unicef-irc.org/children-with-disabilities>.

compliance with the key values and principles that may find in specific procedures and workflows a new methodological approach to assess the impact of a given solution and application on users' fundamental rights.

In research, development, and innovation, the methodology consists of the identification of technical specifications, solution development, and assessment in terms of acceptability and usability among users, the same workflow could be validated by associating to each step an impact assessment in order to define legal requirements, to identify (and maintain coherent) roles and responsibilities within the organizations involved in each step of the development, to design training requirements for users considering their grounds of vulnerability, and share awareness pursuing pre-determined goals for the other relevant stakeholders in order to better harmonise the introduction of the digitalization in the given supply chain.

The iteration of a similar life-cycle describes a new standard of professional diligence that might be considered as a general obligation to addressing vulnerabilities in the given scenario beyond the existence of specific enforceable regulatory tools, setting legal obligations to comply with. In fact, like the technical standards, also the ethical and legal ones might just be globally absorbed in the development cycle and market placement as a pre-requirement to pursuing shared values and needs with the objective to achieve a more inclusive and non-discriminatory society to boost the data economy.

From Digital Vulnerability to Data Anxiety: The Situation of Employees in Digitally Permeated Workplaces

Isabelle Wildhaber, Isabel Laura Ebert

A. Introduction

People may perceive digital data with a sense of fear or «data anxiety» regarding data security, surveillance practices or power relationships. Such anxieties demonstrate how «digital data is rarely thought of by its everyday users as safe, easy to access or manage, or, in the case of personal data, necessarily accurate.»[1] In that sense, digital vulnerability can be seen as a useful concept to capture the fluid and multilayered nature of the human condition when opposed to digitally permeated spaces. Digital vulnerability as a conceptual basis allows us to question the adequacy of some foundational legal and policy norms regarding the situations of employees in digitally permeated workplaces.

This chapter contributes to identifying the factual conditions in which digital technologies might prove disruptive and challenging for people in workplace settings, and in assessing under which conditions, how and to what extent the notion of digital vulnerability might be translated into claims for special legal protection at work. Employees have always been vulnerable in their contractual relationship with their employers, which is why in most countries the employment contract is heavily regulated[2] and contractual autonomy is limited in employment contracts to compensate the perceived inequality of the two contractual parties. In times of digitally permeated workplaces, the vulnerability of employees increases as they become subject to monitoring and control practices by digital technologies.[3]

1 Sarah Pink, Debora Lanzeni and Heather Horst, 'Data anxieties: Finding trust in everyday digital mess' (2018) 5 Big Data & Society 1.

2 Brishen Rogers, 'Workplace Data and Workplace Democracy' (2022) 6 Geo L Tech Rev 454.

3 Isabel Laura Ebert and Isabelle Wildhaber, 'Privacy in the Workplace: A Human Rights Due Diligence Approach' in Jonathan Andrew and Frédéric Bernard (eds), *Human Rights Responsibilities in the Digital Age: States, Companies and Individuals* (Oxford Hart Publishing 2021).

Employees can barely structurally resist or circumvent being subject to digital monitoring or control. Digital vulnerability of employees makes it necessary to reflect upon future changes to national employment laws and to corporate due diligence processes to protect employees from the exposure to harm that might arise from interaction with digital technologies and to address employees' digital vulnerability.

Digital vulnerability is entering into employment relationships via new, data-based forms of algorithmic management. Algorithmic management tools collect data about employees in large and granular quantities to evaluate them in real time or at high speed with the help of algorithms. This results in correlations and metrics on myriad variables about the individual employee.[4] Components of workers' social and organizational lives are transposed into numerical data by technologies with the aim to increase efficiency.[5] Depending on the contextual set-up, there is a high risk that algorithmic management may constitute a new form of surveillance, increasing the digital vulnerability of employees.[6]

Algorithmic management systems combine traditional employment data (e.g., performance appraisals, sick days, or salaries) and new data (e.g., social media activity logs, sensor data, consumer data from GPS or tracking systems) to create processes for identifying, recruiting, retaining, and rewarding job candidates as well as employees. They promise to optimize operations, increase efficiency and innovation, the improvement of employee satisfaction, the reduction of prejudices in decision-making processes, or more objectivity and diversity within the company.[7]

Algorithmic management systems are applied in a range of areas, such as employee selection/recruitment, performance management, compliance management, employee retention and development, work and workplace

4 Isabelle Wildhaber, Melinda Florina Lohmann and Gabriel Kasper, 'Diskriminierung durch Algorithmen–Überlegungen zum schweizerischen Recht am Beispiel prädiktiver Analytik am Arbeitsplatz' (2019) Zeitschrift für Schweizerisches Recht I 459, 461 ff.

5 Kenneth Cukier and Viktor Mayer-Schoenberger, 'The rise of big data: How it's changing the way we think about the world' (2013) 92 Foreign Aff 28.

6 Isabel Ebert, Isabelle Wildhaber and Jeremias Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection' (2021) 8 Big Data & Society 1.

7 Ifeoma Ajunwa, Kate Crawford and Jason Schultz, 'Limitless worker surveillance' (2017) California Law Review 735, 743; Roger W Reinsch and Sonia Goltz, 'Big Data: Can the attempt to be more discriminating be more discriminatory instead' (2016) 61 Louis ULJ 35, 46; Rebecca J Wilson, Kiley M Belliveau and Leigh Ellen Gray, 'Busting the black box: Big data, employment and privacy' (2017) 84 Def Counsel J 1, 32.

design.[8] While electronic employee surveillance has been criticized by scholars since decades, algorithmic surveillance as a modern form of employee surveillance differs from traditional electronic surveillance in the workplace by three factors: (1) variety of data, (2) interoperability between systems, (3) increasing analytical performance of the systems.[9] These factors contribute to the increase of digital vulnerability of employees. As a result, employers now enjoy near-plenary powers to monitor and control workers in the worksite and often during non-work hours as well.

In this chapter, we refer to algorithmic management systems or to «Automated Decision-Making Systems», in short ADM systems.[10] ADM systems are used to predict, recommend, influence, or decide about humans. In most systems, a human still monitors, overrides or decides (decision-support systems with a "human in the loop" and only partial automation).[11] However, qualitative empirical evidence from our recent research project shows that people generally adhere to the suggestions of an algorithmic management system and only occasionally and with reluctance actively reject and override these suggestions.[12] This shows that it does not matter whether we deal with a system that is decision-making (in the sense of art.

8 Isabelle Wildhaber and Gabriel Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz' in Roland A. Müller and others (eds), *Festschrift für Wolfgang Portmann* (Schulthess 2020), 759; Gabriel Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts', (Universität St. Gallen 2021), 42 ff.

9 Wildhaber, Lohmann and Kasper, 'Diskriminierung durch Algorithmen–Überlegungen zum schweizerischen Recht am Beispiel prädiktiver Analytik am Arbeitsplatz', 463; Wildhaber and Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz', 758 ff.; Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, 71 ff.; Kirstie Ball, 'Workplace surveillance: An overview' (2010) 51 Labor History 87.

10 European Law Institute, 'Guiding Principles for Automated Decision-Making in the EU' (2022) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf> accessed 26 October 2023, 8.

11 algo:aware, 'State-of-the-Art Report | Algorithmic decision-making' (2018) <https://actuary.eu/wp-content/uploads/2019/02/AlgoAware-State-of-the-Art-Report.pdf> accessed 26 October 2023, 7 and 11; Jeremias Adams-Prassl and others, 'Regulating algorithmic management: A blueprint' (2023) 14 European Labour Law Journal 124, 20 ff.

12 Isabelle Wildhaber and Isabel Ebert, 'Piercing the Veil of Opacity: Responsibility and Liability for People Analytics Tools at the Workplace' (2022) 1 Morals & Machines 40.

22 GDPR) or one that is only decision-suggesting, in both cases there is significant impact on the employees affected.

In order to portray empirical insights about workplace practices around digital technologies and its impact on employees, this chapter depicts quantitative data about the uptake of algorithmic management tools in Switzerland, as well as a deep dive into qualitative data from case studies that demonstrate the interactions of employees, their supervisors and digital technologies at the workplace, and how it impacts employee perceptions of digital vulnerability (B.). Building on empirical evidence, the chapter sketches several avenues for solutions, both on the legal level through the strengthening of collective worker representation and grievance mechanisms (C. and D.). The chapter also addresses key ethical aspects and proposes better processes to uphold duty of care towards employee well-being at the company level (E.). By showing empirical insights into impacts of current digital workplace monitoring practice on employee vulnerability, this chapter aims at contributing to identify how to reduce digital vulnerability of employees in digitally permeated workplaces.

B. Empirical insights about employee vulnerability in digitally permeated workplaces

This chapter builds on insights gathered as part of our research project «Big Brother in Swiss companies? Trust, data and privacy at work», funded by the Swiss National Science Foundation from 2017 to 2021.[13] The data consists of an empirical quantitative survey from a Switzerland-wide survey on the use of ADM systems in the workplace (2018, 2020), as well as five qualitative case studies in big Swiss corporations (2020, 2021). For reasons of confidentiality, the data is only presented in aggregated and anonymous form. We have specifically processed and reviewed our empirical data for the purpose of emphasizing the aspects of digital vulnerability found in it.

13 <https://www.nfp75.ch/de/rWt7Xm4jTGt4imB7/projekt/projekt-weibel> accessed 26 October 2023.

I. Results from a quantitative survey in Swiss companies

The results of the Switzerland-wide quantitative survey, primarily aimed at those responsible in human resources (HR) departments, are described in the following. In 2018, we conducted an online survey in which 158 large Swiss companies took part, in which these companies were asked whether they use certain IT-based tools for algorithmic people management.[14] 35.4% of participants reported not using any of these tools, while 64.6% used such tools. The online survey was repeated in 2020.

The results of the comparison of the first survey in 2018 and the repeat survey in 2020 showed the current maturity of datafication in the Swiss workplace. The biggest trend comparing the 2018 survey to the 2020 survey was an 18% increase in *Hiring & Recruiting* tools. The 2020 survey found that 39% of Swiss companies included in the survey use partially automated analytics tools to make an initial selection among applicants. Sometimes a tool is used to manage the recruiting process (e.g., reminder of applicant waiting time, automatic conversation). For applicants, in very few cases psychological tests are combined with pattern and speech recognition in applicant files. Algorithmic management tools are most widespread in the area of *Retention & Transition* (63% in 2020), with an increase of 2% compared to the first survey in 2018. Algorithmic management tools with less complex algorithms are used most often. More complex algorithms are mainly used for further processing of analogously collected employee data, for example in the context of linking in HR dashboards. Many low-tech versions of online surveys are used, sometimes as pulse surveys and even more rarely as employee experience dashboards. *Performance Management* tools are in second place (47% in 2020), up 10% from 2018. For example, automated tools for tracking keystrokes and internet usage are widespread, and some companies have begun to use time analysis tools. In terms of *Compliance Management* and *Work & Workplace Design*, there were no major changes between the 2018 and 2020 surveys: Compliance Management saw only a slight overall increase of 4% to 22% in 2020; Work & Workplace Design saw an overall decrease of 2% to 36% in 2020.

It is interesting to note that the 2018 quantitative survey also revealed that most companies do not involve external stakeholders in the design and use of algorithmic management tools. Only 5% of respondents involved busi-

14 Wildhaber and Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz', 764 ff.

ness associations, 8.8% involved business owners, 10.5% involved unions, 28% involved academics, and no companies reported working with civil society. Peer-to-peer exchanges (50.9%) and involvement of consulting firms (59.6%) were the most prominent external stakeholders involved in the design and use of algorithmic management tools. In general, apart from peer-to-peer and consulting companies, there is little exchange with external stakeholders, so that independent expert knowledge is only used by a few companies. Hence, external expertise on creating a workplace for employee well-being and for reduction of digital vulnerabilities is not structurally taken into consideration.

II. Results from the five qualitative case studies in Swiss multinational companies

In the context of the already sketched quantitative developments around the use of workplace monitoring technologies in Swiss companies, the qualitative empirical analysis, as presented in the following, can provide additional insights into aspects of digital vulnerability of employees at the workplace.

The qualitative case studies were carried out in five large Swiss corporations with 20-25 employees and managers between 2018 and 2020. The expert interviews were conducted with employees as well as managers and business strategists. In analyzing the qualitative data for this chapter on digital vulnerability, the focus was on the question of how employees are involved in the design of ADM systems, how they can voice concerns and whether such concerns are taken into consideration, and how this relates to the more general processes for introducing and developing ADM systems. We analyzed the interviews with broad thematic coding.[15] The results are presented below.

To provide more context, in our qualitative case studies, ADM systems were used to plan routes in the logistics industry and to monitor driving behavior in terms of compliance with road traffic regulations and as an incentive to save fuel. Other examples of use in service companies were ADM systems for career planning and identification of talents in the internal personnel pool, or work process-accompanying ADM systems for customer management or claims processing in the insurance industry.

15 Matthew B Miles and A Michael Huberman, *Qualitative data analysis: An expanded sourcebook* (Sage Publications 1994).

1. Information

In some companies, interviewees reported that information about ADM systems could be found on the intranet, but that the introduction of ADM systems was not actively accompanied by a communication process. Therefore, many employees felt poorly informed or did not know exactly what the ADM systems measured at what time and in what way, and what decisions were made on the basis of these measurements or later analyses based on the measured values.

In other companies, a pilot project was launched before the official introduction of the ADM systems. Within this pilot project, companies created an informal mechanism for employee representation. The pilot teams worked, among other things, with so-called power users who came from the workforce and were supposed to educate the teams about the digital technologies that were being used. These power user employees acted as a point of contact for potential suggestions for improvement, praise, criticism, and complaints from the workforce regarding the implementation of the ADM system. However, it was often not obvious to what extent and in what way these insights from the pilot projects influenced the later, organization-wide implementation. The process as such could not claim to be a formal process under labour law.

Other companies launched large-scale culture campaigns on the handling of data in general, and widely distributed information on algorithmic management tools in particular. Many employees perceived this as positive and as creating transparency and making them feel less vulnerable. As a result, employees were on average better informed than in companies where only non-targeted information was available on the intranet without being actively communicated.

Particularly in the introductory phases of the technology, many employees often felt caught off guard or there were methodological problems, i.e., the metrics that were supposed to be recorded were not really collected in a targeted manner. In part, newer technical versions therefore brought better acceptance, but even these «teething troubles» could not be fully addressed, and employees felt digitally vulnerable and punished for technological bias and/or inaccuracy.

2. Consultation

In our case studies, the way in which information was provided affected employees' potential for consultation and for reducing their digital vulnerability by voicing concerns or asking for adaptations. Additionally, if employees had fundamental problems understanding data processing and the scope of ADM systems, they could not participate in consultation processes in an informed manner.

In certain companies, one individual (power user) acted as a kind of guiding figure and contact person for the implementation of ADM systems, but no formalized process for complaints or suggestions or criticism existed. Feedback loops regarding complaints or concerns were very rarely mentioned or described. The fact that feedback during the introduction process is carried out in some companies through informal channels makes the consultation process very informal («casualization»). At the same time, informal feedback cultures could lower the perceived threshold for giving genuine feedback. Such informal processes are far removed from participation respectively information and consultation in the labour law sense. Communication along successive introductions of beta versions and a start-up mentality cannot replace a more formal collective participation mechanism for making employee voices heard. In addition, consultations at the collective level were extremely rare, although they would be more appropriate to the systematic nature of the widespread use of ADM systems.

A participation possibility was mostly made possible either through pilot projects, or through the individual contact of employees via the respective manager. Some companies have introduced employee participation in pilot projects: For instance, one manager explained that «*employees are involved early on when it comes to various, or all, issues that affect employees. We have a very active exchange. It starts with the planning of structural changes, the conversion of fixed workstations to open-plan offices with shared use, and so on. Employees are always involved in issues at an early stage*». This is an example of how pilot projects can be designed and implemented with employee participation, and for ensuring employees can express concerns about set-ups/situations that are digitally mediated and make them feel vulnerable. However, these processes cannot fully substitute for formal collective participation for scaling the use of ADM systems after the pilot phase is complete, as they can never reflect the diversity of the entire workforce's day-to-day work.

3. Data protection law as a buffer against the inappropriate use of ADM systems

For some ADM systems, data protection law did not permit data collection, and/or processing in specific use cases. As a result, sometimes, data protection law functioned as employee protection. This includes applications of ADM for which the purpose-specific data requirement is not met, because personal data is used for several purposes. Here, not only the prior information/consent of the data subject was missing, but there was also a lack of the necessary purpose limitation.

However, data protection law should not be the only method to strengthen protection as the possibilities for objection in data protection are individual in nature and not collective, hence collective effects at scale for reducing employee vulnerability are minimal.

4. Attribution of responsibility and exercise of power

In many scenarios, ADM systems reinforce the hierarchical power asymmetry between supervisors and employees.[16] In addition, qualitative empirical evidence from our research project shows a mismatch in the attribution of responsibility with respect to ADM-based decisions. From the employees' point of view, a clear responsibility is attributed to the supervisor («*clearly the boss is responsible for this*»). At the same time, from the supervisor's point of view, the responsibility is predominantly shifted away to «the machine» («*I can't do anything about it, it was technically determined*»). This can lead to a diffusion of responsibility, which is very problematic in this power constellation and this dependency relationship regarding performance evaluation, and the heightened digital vulnerability of employees.[17] Our empirical findings confirm the discussion in the literature and suggest that ADM systems reinforce the power imbalance between managers and employees.[18]

16 Katherine C Kellogg, Melissa A Valentine and Angele Christin, 'Algorithms at work: The new contested terrain of control' (2020) 14 Academy of Management Annals 366.

17 Simon Schafheitle and others, 'The Bermuda Triangle of Leadership in the AI Era? Emerging Trust Implications from Two-Leader-Situations in the Eyes of Employees' (2020) in HICSS.

18 Will Sutherland and others, 'Algorithmic management in a work context' (2021) 8 Big Data and Society.

5. Communication as a means to engage employees

Some companies have implemented several internal communication tools to improve employee awareness and digital literacy across all departments. One employee explained: «*I think that's also a communication problem when you just say 'this and this is the goal' and you don't address their (employees') fears, you just let it simmer a little bit. Then the rumors start like 'this is automation'*.» Ideally, both employers/supervisors and employees are on the same page when it comes to understanding the core objectives of using ADM systems, which can contribute to the development of a common understanding within the organization and reduce perceptions of digital vulnerability on the sides of the employees. As described earlier, this was not the case in all companies: instead, some companies relied on uploading documents to the intranet without a corresponding accompanying information campaign to raise awareness across the workforce.

6. Learning culture vs. sanctioning culture

Our interviews revealed that the way in which digital technologies are implemented and managed in workplace monitoring plays a key role in whether ADM systems become an empowering tool or whether a culture of sanctioning emerges as result of digital technology use. Workers interviewed offered insights into the sometimes unrealistic expectations assigned to the capacity of digital technology, which measures the exact time it takes a worker to complete their activity, such as delivering goods, and does not take into account other factors that might affect time (e.g., weather or traffic). For example, interviewed workers reported that supervisors ask their workers, «*What have you done in these 8 minutes? It is 30 meters from this house to that house, it should take 30 seconds*.» Employees reported that some measurements were also inaccurate, e.g., the technology did not account for a reduction in speed when road conditions were snowy and icy. Despite inaccurate results, disciplinary action was sometimes taken against employees. In such cases, the technology punishes employees instead of empowering them to work more efficiently or safely/carefully.

The ability to contextualize technical measurements was not necessarily a given in most of the companies surveyed, and in some cases was patchy. Nevertheless, some companies were making efforts to improve the culture to link technology to a learning culture, with so-called data culture initiatives or data culture boards. Supervisors that had an increased level of

awareness of the need to contextualize technology use paid attention to the level of inference, for example, saying «*We want a culture of error, not a command tone, we want people to learn from their mistakes - we don't want people to feel exposed*».

In the companies that invested heavily in establishing an «error culture», supervisors and employees viewed the metrics from the ADM systems primarily as a basis for discussion in their regular performance evaluations and felt less vulnerable to be punished for technological shortcomings. Other companies, on the other hand, considered the readings to be irrevocable and took negative consequences for employees for non-compliance, even if the accuracy of the technological track record was poor, e.g., penalizing them for driving too slowly and using low gears when driving on icy, snowy roads, even if that was the responsible behavior in that very situation.

7. Acceptance of ADM systems

The acceptance of the use of technology by the employees was promoted by the learning culture, the possibility of participation, as well as careful information and communication that was prepared in a way that was appropriate for the target group. The acceptance is also an opportunity to increase the effectiveness of the use of ADM systems, for example, since, according to our studies, a low level of acceptance led to tricking by employees and thus negatively influenced the measurement quality, i.e. the data input often no longer represented the measurement value that was originally intended to be collected.

C. National and international legal foundations

I. National legal foundations

In national laws, there are commonly several applicable regulations that usually apply to the use of ADM systems: Data protection law, employment law, health and safety regulations, privacy protection, employee participation and discrimination protection.[19] Our empirical quantitative studies have shown that many prerequisites of national laws are not fulfilled in

19 Ebert, Wildhaber and Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection'.

practice. Also, legal greyzones exist when it comes to employees' rights where ADM systems are being used. Furthermore, there are many regulatory gaps due to information asymmetries, increase in privacy harms, algorithmic discrimination, or lack of human agency.

Illustratively, in the context to our empirical data, according to Swiss employment law (art. 328b Code of Obligation) the processing of personal data at the workplace requires that the data is workplace-related. However, our research showed that 3% of employers collect non-occupational data from their employees and 7% of employers collect non-occupational data from their job applicants.[20] According to Swiss workplace health and safety regulations (art. 26 Ordinance 3 to the Labour Act) surveillance systems to control employee behaviour are prohibited. However, 22% of all employers do observe employee behaviour.[21]

Adding to this, according to the Swiss Federal Act on Data Protection (art. 19), the collection of personal data and the aim of the collection has to be transparent to the concerned person. However, only 53% of employees understand which input the employer analyzes.[22] The required employee consent must be informed (specific and adequate) and voluntary (art. 6 and 7). Our quantitative empirical studies have shown that 59% of employers ask for a general consent in the employment contract, 27% of employers ask for a specific consent for each use of a tool, 11% do not ask for consent.[23] Therefore, some ADM applications we analyzed were outside the scope of the applicable law.

And finally, according to the Swiss Participation Act (art. 10 lit. a) collective participation is often necessary for the introduction and implementation of algorithmic management tools. Yet, this is not happening in practice: Employee representations and trade unions are only involved as external stakeholders in the design and use of ADM systems in 10.5% of cases.[24]

Summing up, the use of digital technologies at the workplace in Switzerland is currently not fully guided by the legal foundations and some companies seem to be consciously or non-intentionally taking legal risks, as well as implementing ethically questionable practices.

20 Wildhaber and Kasper, 'Quantifizierte Arbeitnehmer: Empirische Daten zu People Analytics in der Schweiz', 767.
21 ibid, 768.
22 ibid, 769.
23 ibid, 769.
24 ibid, 770.

II. International legal foundations

Regarding workplace law issues, national legal foundations are predominant. Labour law and employment law traditionally belongs to the regulatory sovereignty of the state concerned. Across Europe, however, with respect to data protection issues, EU data protection law, in particular the GDPR, as well as national laws of the member states (art. 88 GDPR) should be consulted.[25] Equally, for the European context and related to data protection, Convention 108 of the Council of Europe is relevant. Convention 108 is the first binding but not directly applicable treaty on data protection.[26] The Convention aims to protect the right to privacy in the automatic processing of personal data (art. 1 Convention 108). To this end, the Convention provides a set of data protection principles, as well as instructions for cooperation between the Parties in the implementation of the Convention. The Convention applies to automated data collections and files and to automated processing of personal data in both the public and private sectors (art. 3 para. 1 Convention 108).[27]

Globally, the protection of privacy rights between private individuals is protected by the International Covenant on Civil and Political Rights (UN Covenant II). Art. 17 protects against arbitrary or unlawful interference with private life, family, home or correspondence, as well as against unlawful impairment of honor or reputation.[28] With regard to the participation rights of employees, a wide variety of provisions of international law must be considered. For example, the European Convention on Human Rights (ECHR) must be taken into account. Art. 8 European Convention on Human Rights (ECHR) establishes a human right to respect for private and family life. According to the case law of the European Court of Human

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 (2016); Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, 109ff.

26 Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'CETS No. 108' (1981).

27 Kasper, 'People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, 130.

28 United Nations, International Covenant on Civil and Political Rights (ICCPR) (1976).

Rights (ECtHR), the term private life can also include professional activities.[29]

The protection of the employee health is an obligation under international and constitutional law. These obligations are anchored, in particular, in art. 6-8 (right to healthy and safe working conditions) of the International Covenant on Economic, Social and Cultural Rights (ICCPR or UN Covenant I). In June 2022, health and safety at work was declared a fundamental principle of the International Labor Organization (ILO).[30] The basic principles of the ILO were developed in ten conventions. The recognition of health protection as a further fundamental principle means that ILO Conventions 155 and 187 now have the status of core labour standards and thus of universally valid human rights.[31] They thus constitute a minimum standard below which all ILO member states may not fall. With ILO Convention 155, the member states undertake to pursue a national policy of preventing accidents and damage to health that occur as a result of or in connection with work (art. 4 para. 2 ILO 155). The more recent ILO Convention 187 supplements the provisions of ILO Convention 155 and aims to specify the implementation of the prevention of accidents or damage to health in the context of work.

In the Community law of the European Union, great importance is attached to the protection of the health of employees. This is reflected in the recitals of Council Directive 89/391 of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers. The Organisation for Economic Co-operation and Development (OECD) has also published a number of principles that are relevant to the use of ADM systems. The OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD MNE Guidelines) stipulate, for example, an anti-discrimination requirement, according to which companies should be guided by the principle of equal opportunities and equal treatment in the activity of employing workers. Furthermore, section V para. 3 of the OECD Guidelines stipulates a duty of consultation and

29 BĂRBULESCU v. ROMANIA App no 61496/08 (ECHR), Recital 71.

30 International Labour Organization, 'A safe and healthy working environment is a fundamental principle and right at work' 2022) <https://www.ilo.org/global/topics/safety-and-health-at-work/areasofwork/fundamental-principle/lang--en/index.htm> accessed 26 October 2023.

31 International Labour Organization, 'ILO Declarations' <https://www.ilo.org/global/about-the-ilo/how-the-ilo-works/organigramme/jur/legal-instruments/WCMS_428589/lang--en/index.htm> accessed 26 October 2023.

cooperation on the part of the employer vis-à-vis the employees or their representatives in «matters of common interest».[32] The UN Guiding Principles on Business and Human Rights (UNGPs), discussed in the following, are consistent with the OECD Guidelines. In addition, the OECD has published recommendations on the use of artificial intelligence in 2022. In these, the OECD points out that the use of AI in companies must, among other things, respect internationally recognized employee rights, data protection and anti-discrimination.[33] In a similar vein, the UNGPs encompass the technology sector. Broadly speaking, the Business & Human Rights framework is centered around the UNGPs. The Business & Human Rights Framework outlines the State duty to protect against human rights abuses stemming from or being linked to company activities, and businesses' responsibility to respect human rights, and to provide remedies for individuals who have been harmed by business activities.[34] The UNGPs consist of 31 guiding principles, which are structured into three pillars that provide a framework for governments and businesses to protect and respect human rights. The three pillars are: (1.) the State duty to protect human rights, (2.) the corporate responsibility to respect human rights, and (3.) access to remedy. The UNGPs provide a framework for businesses to identify, prevent, mitigate, and remedy human rights impacts associated with their operations, products, and services, and are widely recognised as the authoritative international standard for responsible business conduct, along with the OECD MNE Guidelines.

The central concept of this corporate responsibility towards people and their rights is the company's human rights due diligence, which is based on the logic of operational risk management processes, but specifically on risks to people, and thus also on the rights of employees. The UNGPs are frequently referenced in corporate policies and processes because they are based on the universally recognized framework of human rights and enshrine the "minimum standard for responsible behavior" by private companies. The UNGPs are implemented by a large number of global

32 OECD, 'OECD Guidelines for Multinational Enterprises on Responsible Business Conduct' <https://www.oecd-ilibrary.org/content/publication/81f92357-en> accessed 26 October 2023.

33 OECD, 'Recommendation of the Council on Artificial Intelligence' <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 26 October 2023.

34 OHCHR, 'Guiding Principles on Business and Human Rights' (*United Nations,* 2011) <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 26 October 2023.

corporations and are increasingly reflected in national legislation and national policy packages. Switzerland has also committed to implementing the UNGPs, including within the framework of a National Action Plan for Business and Human Rights. France passed the "loi de vigilance" (Duty of Care Act) in 2017, and in Germany the Supply Chain Due Diligence Act came into force on January 1, 2023. On 25 July 2024, the European Union adopted a directive on corporate sustainability due diligence (Directive 2024/1760), that also builds on the UNGPs.

There is, of course, also the possibility of dealing with adverse impacts on human rights being linked or stemming from business activities through non-legal means in the form of the mediation processes of the so-called National Contact Point for Responsible Business Conduct of the OECD, which can be found in each member state of the OECD.

Context-specific ethical approaches, e.g. for the context of digital technologies at the workplace, can be combined with the UNGPs insofar as the UNGPs show the minimum standard that can be expected and take contextual factors into account when exercising the duty of care. These due diligence obligations are therefore obligations to establish certain systems and processes in companies in order to identify, address and mitigate adverse impacts on human rights, and to help those affected in the event of complicity or involvement in human rights abuses.

The UNGPs stipulate that companies establish processes through which they identify and address human rights risks and through which they take measures to reduce or, ideally, eliminate these risks. Broadly speaking, the human rights due diligence process can be divided into four steps[35]:

a. Identify and assess the impact of business activities on human rights in order to assess the nature and extent of human rights risks;
b. Act to prevent and mitigate human rights risks, including through integration into internal functions and processes;
c. Track the effectiveness of risk mitigation measures over time;
d. Adequate communication of measures to address human rights impacts.

Structuring the due diligence responsibilities along the UNGPs is helpful for implementation in the company when using ADM systems in the work-

35 B-Tech, 'Key Characteristics of Business Respect for Human Rights' (*United Nations Human Rights Office of the High Commissioner,* 2020) <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/key-characteristics-business-respect.pdf> accessed 26 October 2023.

place. The human rights affected may include the right to privacy, the right to non-discrimination or the right to health. However, the UNGPs recommend an analysis in relation to all human rights and a prioritization of measures based on the possible severity of a human rights impact («severity»).[36] Human rights due diligence will look different in various organizations and contexts. However, certain features of human rights due diligence are particularly important when addressing human rights risks related to technology products, services and solutions.

The UNGPs have established themselves as a global standard for corporate responsibility and are used by many large technology companies, which is evident, among other things, based on publicly available risk analyzes and reports. For example, the multi-stakeholder organization Global Network Initiative regularly reviews the implementation of the UNGPs in its member companies.[37] Employees affected by companies headquartered in an OECD member state can initiate mediation proceedings at the respective National Contact Point for Multinational Companies.

Lastly, consider the UN Sustainable Development Goals (SDGs). The eighth goal is dedicated to promoting inclusive and sustainable economic growth, employment and decent work for all. The eighth goal is divided into 12 sub-categories - Goal 8.8 reads, «Protect labour rights and promote safe and secure working environments for all workers, including migrant workers, in particular women migrants, and those in precarious employment».[38]

36 B-Tech, 'Taking Action to Address Human Rights Risks Related to End-Use' (*United Nations Human Rights Office of the High Commissioner,* 2020) <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/taking-action-address-human-rights-risks.pdf> accessed 26 October 2023.

37 Global Network Initiative, 'Company Assessments' <https://globalnetworkinitiative.org/company-assessments/> accessed 26 October 2023.

38 United Nations Department of Economic and Social Affairs, 'Goal 8: Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all' 2015) <https://sdgs.un.org/goals/goal8> accessed 26 October 2023.

D. Suggestions to address regulatory gaps in digital vulnerability of employees

The majority of ADM systems are operated with a human still monitoring and possibly overriding the ADM system (human in the loop).[39]. At the same time, our qualitative case studies showed that humans usually stick to the suggestions of the ADM system, and only actively reject and override these suggestions sporadically and with restraint. In fact, most employees followed the ADM-based suggestions, so it is very likely that human decision-making was predetermined. A "human in the loop" is therefore not enough to ensure that the output of an ADM system has significant negative effects on the people about whom the decision is made and that a human assessment of the facts actually takes place.

I. Strengthening collective participation

Employees are the main "data providers" of ADM systems at the workplace. One of the main tasks of employees and their representatives is to create a counterweight to the prerogatives of employers and to address collective risks and damages within the framework of social dialogue. Strengthening the rights of employees, their representatives and unions is therefore an evident option. The employer must be obliged to inform its employees not only individually (as in data protection laws) about ADM systems, but also collectively. Collective participation rights must exist in the development, procurement, configuration and use of ADM systems as well as in all changes to the ADM system or its configuration that affect, or are likely to affect, working conditions. Furthermore, ADM systems must become an important topic of social partnerships.

This could be accomplished as follows, whereby the suggestions listed here are to be understood as a possible sample of options and as non-exhaustive:

1. Given the complexity and opacity of ADM systems, employee representatives can only fulfill their tasks if they receive transparent, precise, understandable, relevant and timely information about the planned deploy-

39 Wildhaber and Ebert, 'Piercing the Veil of Opacity: Responsibility and Liability for People Analytics Tools at the Workplace', 43; Adams-Prassl and others, 'Regulating algorithmic management: A blueprint', 20ff.

ment, intended use, expected impacts and operation of ADM systems. This also serves transparency. The employee representatives need information about the actors involved (developers, implementing positions within the company) and about any impact assessments, potential risks and planned risk minimization measures. It is important that all information is communicated in a format that is understandable, comprehensible and appropriate to the expertise of the recipient. To ensure that the information does not become too long to absorb for the individual or is overloaded with "meaningless" information, the legislature could set requirements for the type, clarity and scope of the information that must be included.

2. In order to ensure meaningful participation of employees and their representatives, ADM systems should be expressly included in the scope of existing collective participation rights.
3. Mandatory constitution of employee representation with collective rights (not the case in Switzerland, for example).
4. Institutionalized cooperation between the employer and the workforce in the form of a commission for occupational health and safety and for participation, made up of equal numbers of members of the employee representatives and the company management. One could also form additional appropriate personnel representations and give them effective participation rights to ensure the participation of employees in relation to ADM systems and data processing.
5. Explicit right of the employee representatives to consult an internal or external expert (as provided for by German law[40]).

II. Continuously enabling employee objections

The opportunities for employees and their representatives to lodge objections regarding ADM systems must be improved. This could be achieved, for example, through the following measures:

1. Clarification of the employee representatives' right of action, i.e. the employee representatives should have the capacity to be a party and to litigate or have partial legal capacity and to conduct collective legal disputes and to submit collective complaints on behalf of groups of employees.

40 §80 para. 2 and 3 *Deutsches Betriebsverfassungsgesetz*.

2. The financing of collective complaints would also have to be regulated.
3. Granting employee representatives access to, or insight into, processed data would help reduce the flood of information at an individual level. Thus, we propose the right of employees and their representatives to access all individual-level data collected, used, processed or created by ADM systems (provided that the data subjects consent), as well as the right to transfer the data in a structured, common and machine-readable format, as known in art. 20 GDPR.
4. Sanctioning a violation of the right of participation through administrative-criminal fines.
5. Protection against dismissal or no acceptance of unfair dismissal if employees refrain from using or participating in the development of ADM systems.
6. Better collective enforcement could be achieved through intervention by labour inspectorates.

III. Structures for oversight and control/enforcement

The suggestions listed here are to be understood as a possible and non-exhaustive sample of options for structures for supervision and control:

1. Mandatory anchoring of corporate due diligence obligations (see V.) regarding the establishment and implementation of risk identification and risk management.
2. Use of impact assessments before and during the development, introduction and use of ADM systems to keep negative consequences as low as possible, with the involvement of employees or their representatives.
3. Regular reporting ("reporting") and thus transparency about identified risks and measures taken to eliminate these identified risks, including impact measurement, and an accountability report on the effects and the well-being of employees.
4. Creation of appropriate control and supervisory bodies.
5. Strengthening the skills and expertise of the National Contact Points for Responsible Business Conduct, which promotes the OECD Guidelines for Responsible Business Conduct.

IV. Solutions empowering social partnerships

Employee participation in ADM systems does not necessarily have to be initiated by the legislature. Before thinking about revision efforts at the legislative level, it is worthwhile to work out solutions within social partnerships. Social partnerships are able to take conscious actions collectively. Due to their proximity to companies and employees, the social partners are particularly predestined to overcome the challenges of ADM systems in the workplace, in a flexible, effective, quick and socially acceptable manner. For decades, many employers and employees have been regulating the working conditions in their company, industry or economic sector on this company-specific or industry-specific basis. The compromises negotiated are tailor-made, pragmatic and, if necessary, consider the individual needs of the contracting parties.[41]

Collective law instruments can therefore be chosen, such as the interaction of social partnerships, the conclusion of works agreements or of collective bargaining agreements. The central element of social partnerships is the collective bargaining agreement, which is the ideal instrument for meeting the need for flexibility. Collective bargaining about the challenging and unclear aspects of ADM systems in the workplace is genuinely within the very nature of labour law. The individual inferiority of the individual employee is compensated for by the collective and its action. Collective bargaining and the conclusion of a collective bargaining agreement allow a relatively low-threshold, democratically legitimated participation in shaping working conditions in the new world of work.[42] Collective bargaining agreements can therefore represent a key to overcoming the challenges of ADM systems by providing an institutional framework with the aim of appropriately balancing the interests affected. However, it seems that this possibility is not often used in practice and is not very well anchored in the consciousness of companies, which is why there is a need to raise awareness on the subject.

41 Isabelle Wildhaber and Raquel Pais, 'Neue Arbeitswelt und Gesamtarbeitsverträge-Plädoyer für einen Rechtsschutz über die Sozialpartnerschaft angesichts der Herausforderungen der neuen Arbeitswelt' in Claudia Seitz, Ralf Michael Straub and Robert Weyeneth (eds), *Rechtsschutz in Theorie und Praxis* (Helbing Lichtenhahn 2022), 542.

42 ibid.

E. Suggestions to address ethical requirements in digital vulnerability of employees

The restoration of human agency requires a space for meaningful ex ante and continuously on-going/ex post representation of employees in the form of grievance mechanisms regarding the implementation and development of ADM systems. To ensure meaningful participation of affected individuals, ADM systems should be explicitly included within the scope of existing information and consultation rights.[43]

I. Key issues to include in an ethical analysis of workplace monitoring

In the following, the ethical analysis focuses on ADM systems in the workplace, building on the findings from the qualitative empirical case studies, which are supplemented by aspects from corresponding expert literature.

1. Deep Insights into privacy and possible monitoring of employee activities

Data-driven technologies now permeate almost every aspect of business life: our qualitative case studies showed that Swiss employees are in daily contact with or controlled by ADM systems.[44] The impact on employees' privacy is also discussed in the literature as one of the most serious ethical problems of datafication in the workplace.[45]

Although the concept of privacy is expressed in different ways in different legal systems, it protects the right to respect for private and family life, home and correspondence (see art. 8 ECHR). Big data analytics in human resource management have a significant impact on the privacy of employees and may lead to abuses/harms.[46] The right to privacy underpins

43 Adams-Prassl and others, 'Regulating algorithmic management: A blueprint'; OHCHR, 'Guiding Principles on Business and Human Rights'; B-Tech, 'Key Characteristics of Business Respect for Human Rights'.

44 Jean-Philippe Deranty and Thomas Corbin, 'Artificial intelligence and work: a critical review of recent research from the social sciences' (2022) AI & SOCIETY 1.

45 Ebert, Wildhaber and Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection'.

46 Alexandra Mateescu and Aiha Nguyen, 'Algorithmic management in the workplace' (2019) 8 Data & Society 1.

and is closely linked to other fundamental rights in the workplace, such as freedom of association and freedom of speech.[47]

Invasions of the right to privacy can be problematic with respect to participation, particularly when the employer is able to obtain insights into communications and potential mobilization activities of employees in the workplace. A free exchange among employees is hardly possible if communication processes or assembly patterns are monitored.

2. Timing of information and consultation

The employer should consult with employees early in the decision-making process, ideally before a decision is made to introduce ADM systems. The earlier discussed UNGPs call for the structural involvement of affected stakeholders as part of human rights due diligence. This can ensure that employees have a meaningful opportunity to participate in the discussion early in the process when important decisions are made and that their views are considered. Experts also suggest the involvement of independent, ethical expert panels.

Thus, data does not tend to be organized by people in discrete and complete ways that are coherent with the understandings that software designers have of computer systems. Data also does not necessarily fit with processes of audit and governance. Moreover, as is well established in critical data studies[48], data is not an entity with objective meanings that can be stolen. Rather it is contingent, in its meanings and in the ways that it is organized.[49]

3. Data competence / data literacy

To enable employee participation, it is essential that employees have an appropriate level of basic knowledge about data processing, analysis and possible bias effects as consequences. Employee data literacy is critical to informed participation in the use of ADM systems. Only when workers can

47 Christoph Grabenwarter, *European Convention on Human Rights: Commentary* (Bloomsbury Publishing 2014), Art. 8 ECHR N 82.

48 Danah Boyd and Kate Crawford, 'Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon' (2012) 15 Information, communication & society 662.

49 Pink, Lanzeni and Horst, 'Data anxieties: Finding trust in everyday digital mess', 12.

understand and interpret the data collected by monitoring tools can they exercise informed voice in participation processes and gain agency over the use and interpretation of their data.[50]

Illustratively, a study[51] demonstrates that human decisions triggered positive emotion as employees connected human decisions with a possibility of social recognition, while algorithmic decisions had a mixed response in the sense that algorithms were seen as helpful but also offering a tracking possibility. So employees perceive digitally permeated decisions differently from human ones. Equally task characteristics differed,"*in particular, perceptions of whether tasks require more ''human'' or more ''mechanical'' skills significantly influence how people perceive algorithmic decisions compared to human-made ones. With tasks that mainly involve mechanical skills, participants trusted algorithmic and human decisions equally, found them fair, and felt similar emotion toward them, consistent with our hypotheses. While the degree of perceived trust, fairness, and emotion was the same between algorithmic and human decisions, the reasons behind people's perceptions differed. With human-made decisions, participants attributed fairness and trust to managerial authority; with algorithmic decisions, to reliability and the lack of bias. For the human-made decisions, some participants mentioned the manager's social recognition as a factor that could positively influence workers' emotions. For algorithmic decisions, on the other hand, participants mentioned that algorithms could act as tools to help workers complete their tasks, which could positively influence workers' emotions; or workers might feel negatively about algorithms, if they felt they were being watched and monitored.*"[52]

Such studies suggest that it matters greatly for employee perception and for the orgnization's perception of digital vulnerabilities how decision-making and task design is done.

4. Data transparency

Data transparency is an often-discussed factor in enabling employee participation. It is important that employees have access to the data collected

50 Helen Kennedy, Thomas Poell and Jose van Dijck, 'Data and agency' (2015) 2 Big Data & Society 1.

51 Min Kyung Lee, 'Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management' (2018) 5 Big Data & Society 1.

52 ibid, 11.

and in a format that allows them to understand what information is being collected and how it is being used. Companies should ensure that their employees have access to the relevant data and that it is prepared in a format that corresponds to their individual data skills for comprehension. Clear communication of data collection and presentation of how data is handled is a basic requirement so that employees can take part in participation processes. From a technical perspective, it can be complex or impossible to make ADM-supported processes completely transparent, as some technologies are acquired from third-party providers, sometimes from abroad. When using so-called "off-the-shelf" products, the employer does not know exactly which information about employees is measured in which way and what are possible weaknesses of the technology, for example with regard to the measurement quality, because the manufacturer does not provide this information in a completely transparent manner.

5. Clarification about the scope of application of the ADM systems

Since the majority of ADM systems are not developed in-house but are sourced from external providers, this can have an impact not only on data transparency but also on the traceability of decisions. The traceability of decisions must be a core component of an employee participation process.

Clear disclosure of the scope of ADM systems in the workplace is of great importance for employees in order to understand the extent to which they are affected. It is important that employees know in which areas their work is subject to monitoring with the help of ADM systems and what options are available to them to deal with these ADM systems. It is necessary to provide information about which processes, and objection options can be initiated if problems or conflicts arise around the ADM system, both in the introduction process and in daily use.

6. Avoiding «black box systems»

A frequently discussed phenomenon in ADM systems is the genesis of so-called "black box systems".[53] Data-driven ADM systems are being introduced that lack transparency about their decision-making. Employees often must accept extensive data collection about themselves, while the

53 Ifeoma Ajunwa, 'The "black box" at work' (2020) 7 Big Data & Society 1.

details of decision-making are shrouded in secrecy. This can make the employer's ADM-based decisions highly opaque for employees and make it more difficult for them to have a say, as the necessary information base, including consultation, is missing. Employees are thus confronted with a lack of transparency, e.g. regarding discrimination/distorting effects, accountability or explanations about the functioning or even the logic of the "black box" at work.[54] The traceability and fairness of an ADM model can only be achieved through reducing employee vulnerability by ways of technical methods and their communication to employees, so that exchanges about potential for improvement are possible. Here, it is important to rely on collaborative management systems and promote diversity so that different expert opinions make the system more robust and resilient for the benefit of employees, both from a technical, from a labour law and from an ethical perspective.

II. Opportunities at company level to implement due diligence

In general, ethical responsibilities of companies can be derived from the Business and Human Rights Framework, centred around the UNGPs, as described earlier.[55] In addition to the state's duty to protect people from human rights violations by private individuals, the UNGPs postulate a corporate responsibility to respect human rights and to participate in redressing human rights abuses that a company is linked or contributing to. To re-state, the UNGPs have become the de-facto global standard for responsible business conduct and are in line with the OECD MNE Guidelines Enterprises, as briefly sketched prior.

It would be conceivable for the employer to have a duty of care, similarly to the one conceptualized in the UNGPs. This duty of care would include that the employer and the employee representative (or the responsible union) establish a process for exercising human rights due diligence with a focus on the rights of employees at an early stage before the introduction or development of an ADM system. The duty of care would also include regular reporting on the effects on employees based on impact assessments with the involvement of those affected, and an accountability report on

54 Bert Heinrichs, 'Discrimination in the age of artificial intelligence' (2022) AI & society 1.

55 OHCHR, 'Guiding Principles on Business and Human Rights'.

the well-being of employees, as well as measuring the efficiency of the protective measures taken.

The building blocks of the necessary due diligence steps in the context of an ADM system in the workplace are described below and consist of four steps.

1. Identify and assess impacts to assess the nature and extent of human rights

In particular, step 1 of the duty of care is often carried out in the form of a so-called "impact assessments". The impacts of complex ADM systems are often difficult to predict and difficult to manage ex post, so the quality standard must be high, regarding the scope and quality of human rights ex ante and ex post analysis of potential risks of ADM systems as well as regarding the review and implementation of appropriate risk reduction strategies. A thorough internal record of the impacts of ADM systems is important to enable regular impact assessments. This should be done annually or as needed throughout the entire life cycle of a system, and also when additional tools are introduced, in order to avoid negative cumulative effects.

Step 1, derived from the UNGPs for the context of the use of ADMs in the workplace, should include, among others, the following elements:

- Systematic description and assessment of the relevant impacts and risks through reference to qualitative and quantitative information about the use of the ADM systems;
- All "system level" information that is to be made available to employees, and the manner in which it is made available;
- Employers should consult employee representatives and relevant expert groups when identifying the risks and possible protective measures ("stakeholder engagement"). The views of employee representatives and expert knowledge must be taken into account and included. The perspective of those who are potentially severely affected by the impacts should be given appropriate weight. Mandatory collective participation is recommended.[56]

56 Adams-Prassl and others, 'Regulating algorithmic management: A blueprint'.

2. Act to prevent and reduce human rights risks, also through integration into internal functions and processes

The UNGPs were designed to establish a global expectation of responsible business conduct. To this end, the UNGPs require a company to take positive and proactive steps to review, improve and, where appropriate, transform its own business practices and cultures. This also includes the expectation that companies try to encourage employees, business partners and others to act responsibly and with respect for all human rights. When it comes to technology use, this focus on improving new business practices and relationships when dealing with ADM systems in people management is critical.

Step 2 should include, but is not limited to, the following elements[57]:

- Description and assessment of all existing protective measures to mitigate human rights risks in the context of ADM technologies;
- Gap analysis, where existing measures do not cover risks;
- Identification of new measures where gaps have been identified;
- Prioritization of measures according to the "severity of risks".

3. Track the effectiveness of risk reduction measures over time

Companies must assess the effectiveness of their measures to address human rights risks. As a third step in the human rights due diligence process, the UNGPs (UNGP 20) set the following requirement: "In order to verify whether negative impacts on human rights are being addressed, companies should monitor the effectiveness of their response." Follow-up should be based on appropriate qualitative and quantitative indicators and use feedback from both internal and external sources, including affected stakeholders.

For example, a measure could include training by companies for the workforce if ADM systems are used. Targeted training of employees in data analysis and interpretation can help improve their data skills and give them the necessary confidence in dealing with the planned or implemented ADM systems.

57 B-Tech, 'Taking Action to Address Human Rights Risks Related to End-Use'.

Step 3 should include, but is not limited to:

- Impact measurement: Assessment of the effectiveness of new and existing protective measures, including
- Assessment of adequacy: assessment of whether they are appropriate to the impacts and risks;
- Feedback to stakeholders: description of the consultations carried out with employees and their co-workers and disclosure of changes made in response to the views expressed.

4. Appropriate communication of the measures with a view to dealing with human rights impacts

The UNGPs state that companies "should be accountable for the way they manage their human rights impacts" and "be prepared to communicate this externally, particularly when concerns are raised by or on behalf of companies." affected stakeholders" (UNGP 21). The UNGPs state that "communication may take various forms, including face-to-face meetings, online dialogues, consultations with affected stakeholders and formal public reports".

Communication and reporting should focus on the impacts of ADM systems on employees that have been identified. However, communication and reporting must also include transparency about the remedial measures the company has taken to address the impacts and an assessment of the effectiveness of these measures.

Step 4 should include, but is not limited to:

- The impact assessment should generally be communicated publicly, apart from confidential technical and commercial information.
- The impact assessment should be available to employees and their representatives.
- Cooperation with supervisory authorities with appropriate measures to protect confidentiality if irregularities have occurred.

For any disclosure, especially of a public nature, care must be taken to ensure that the information is provided in a suitable manner and format that is easily accessible in order to make it comprehensible.

F. Conclusions

This chapter showed empirical insights about workplace practices around digital technologies and its impact on employees using quantitative and qualitative data about the implementation processes and use of algorithmic management tools in Switzerland. It explored how such practices impact employee perceptions of digital vulnerability. The chapter discussed the key legal foundations on an international level and addressed key ethical aspects and proposed several avenues for solutions.

By showing empirical insights into impacts of current digital workplace monitoring practice on employee vulnerability and proposing matching avenues for solutions, this chapter contributed to exploring how digital vulnerability of employees in digitally permeated workplaces can be reduced. We contextualize the discourse in legal and critical data studies about implications for labour law and ethical challenges.[58]

Further research could explore empirical results from other countries and whether they replicate or differ from the presented data, and to which extent our proposed solutions could help to address the identified digital vulnerabilites of employees.

58 Ajunwa, 'The "black box" at work'; Benedetta Brevini and Frank Pasquale, *Revisiting the Black Box Society by rethinking the political economy of big data* (SAGE Publications Sage UK: London, England 2020); Rogers, 'Workplace Data and Workplace Democracy'; Adams-Prassl and others, 'Regulating algorithmic management: A blueprint'; Ebert, Wildhaber and Adams-Prassl, 'Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection'; Ajunwa, Crawford and Schultz, 'Limitless worker surveillance'.

Design for Agency *vs.* Vulnerability by Design – The Case of Swiss Agriculture

Léa Stiefel, Alain Sandoz

A. Introduction

Should the sensitive data that is shared in an information infrastructure be centralized or distributed? The question appeared openly on the scene of Swiss agriculture in the years 2017-2019. Farmers were producing large volumes of heterogeneous sensitive data for a few hundred private and public organizations that independently collected and used it to provide services. Farmers were increasingly dissatisfied with a situation that was getting out of control. Would it not be better to put all the data in a central database and to delegate control to a unique actor, rather than to distribute control piecewise to organizations that managed subsets of data in many heterogeneous databases? The issue sparked debate and triggered the opposition of two projects, each attempting to establish the foundations of an information infrastructure for agriculture through one of two alternatives: centralization *vs.* distribution.

The question concerns information infrastructures (*II*s) in sectors of activity where digital systems play a significant role.[1] Data is involved in every *operation* executed by a digital system and the transmission of data is involved in every *inter-operation* between any pair of digital systems connected by a network. What if the data represents information *of interest* to a social actor, a person, or an organisation? In all generality, the two digital systems might be *controlled* by different actors, and the actor concerned by the data might be a *third* party. In this situation, information that is possibly sensitive about the third actor is shared by two other actors through their digital information systems. If sensitive information about many actors (possibly tens of thousands or millions) is shared by a small number of

1 Bowker *et al.,* 'Toward information infrastructure studies: ways of knowing in a networked environment' in *International Handbook of Internet Research* (Springer 2009), 97; Monteiro *et al.*, 'Innovation in Information Infrastructures: Introduction to the Special Issue' (2014) JAIS Vol 15; Poppe *et al.*, 'Architecting in Large and Complex Information Infrastructures' (2014) in SCIS, 90.

actors (possibly a few dozens or thousands, each operating a *database*), then questions emerge about who controls and who shares what data, how sensitive data is used and by whom, how it is transformed after having been shared, and how it is re-shared after having been transformed, etc.

The question is not just rhetorical. Digital healthcare, for example, is concerned with the design and implementation of Electronic Patient Records.[2] Standardisation of data in the systems where it originates and it is used have been proposed to stabilize complexity and costs, and improve the effectivity of information management in healthcare *II*s. It is difficult to achieve and faces challenges, *e.g.*, in relation to the usage of patient data by public and/or private healthcare actors.[3]

We examine this question in the *II* of agriculture in Switzerland from the perspective of digital vulnerability, accountability, and trust between actors: data-*owners* (*i.e.*, persons for whom the data is sensitive) and data-*users* (*i.e.*, actors who use and possibly share the data).

The project to centralize data was called Barto and started in 2015. By 2017 an alternative proposition to *manage* data distribution rather than centralize data had emerged and was called ADA. The two projects had radically opposed conceptions of data sharing: a centralized platform with third-party modules for smart-farming in Barto, and a peer-to-peer distributed platform for authorized data-transmission between database operators in ADA. Based on the materials collected during fieldwork in 2018 and 2019, and on subsequent research on software-based platforms, we explore how the vulnerability of farmers, the accountability of organizations, and the trust relationship between the two groups translate in each approach. This brings us to examine trust in relation to digital platforms. To do this, we use a model of organizational trust.[4]

This work is the result of a multidisciplinary collaboration. In January 2018, the first author, then a PhD student in STS (Science & Technology Studies), had just started her thesis and was interested in tracking the dynamics of digitization in Swiss agriculture. She had attended public presentations of both projects and had introduced herself to ADA's archi-

2 Hanseth & Bygstad 'Managing IT in Large Organizations as Platform-Oriented Infrastructures' (2021) <www.researchgate.net/profile/Ole-Hanseth/publication/354435940> accessed 5 June 2024.

3 www.researchgate.net/profile/Ole-Hanseth/publication/35443594

4 Mayer *et al.*, 'An integrative model of organizational trust: past, present, and future' (1995) AMR, Vol 20, 709.

tect (the second author), asking to (ethnographically) follow the project's development.

In September 2018, the terms of a collaboration were defined. In parallel to other enquiries in the sector, the ethnographer would go behind the scenes of ADA to follow and document all of its developments. In return for full access, she would provide the architect with feedback on her observations, according to the rules of her discipline and her progressive understanding of digitization, via anonymized reports of her interviews. The architect would benefit from this informed perspective to drive ADA in its socio-technical environment.

After ADA was put in production in 2019 and the project ended, the authors crossed the boundaries of their respective disciplines (STS and Computer science) to better understand the relationships between architecture and governance in digital platforms. By exploring dependencies, autonomy, symmetry and control, architecture and governance, we have acquired knowledge on digital platforms and produced several small theoretical contributions in STS. In this paper, we intend to explore the platforms ADA and Barto under the perspectives of digital vulnerability, accountability, and trust (noted *dVAT*), three social concepts that were implemented in different ways at the technical level in each solution.

At the end of the nineties, the government needed a system to implement new agricultural policies.[5] There was a political consensus among Swiss cantons and federal authorities on the urgency to build a *database* that would implement the requirements of new international trade treaties.[6] Weak resistance to change by cantonal administrations was more a stance than effective, sometimes justified by technical or organizational reasons. At that time, farmers sent paper forms to their local administrations who employed typists to transcribe the written declarations with digital computers. Controllers would visit farms bringing printouts with values to be checked on site. The Internet and mobile technologies were not yet available. With time, the situation evolved and got out of control. The topic of data sharing then became acute. Section B. describes the context where Barto and ADA emerged. Section C. makes a distinction between the [actor-interaction] and [system-interoperation] relationships that are

5 Sandoz, 'Meeting the Requirements of Agricultural Policy Management on Information Technology' (1999) *EFITA*.

6 <www.parlament.ch/blog/Pages/politique-fait-la-vie-dure-au-lait.aspx?lang=1040> accessed 23 March 2023.

fundamental to understanding digital dependencies, and incidentally of *VAT* in the digital context. Section D. describes methodology and the field materials. Section E. is devoted to the case studies. Subsection E.I. concerns Barto and how it was perceived. Subsection E.II. concerns ADA and describes chosen aspects of its design, how the platform functioned, and how it *intended* to counter what was perceived as a threat, including the loss of accountability perceived by public organizations. Its architecture is more detailed than subsection E.I.. What we know of Barto's design (the project declined an interview by the ethnographer) is classical and documented in the literature generally under the term of *software-based platform*.[7] Section F. discusses how digital vulnerability, trust, and accountability translated in both projects and is followed by a conclusion.

B. Context

In Switzerland, *ca*. 48'000 farms[8] (*i.e.,* - 40% less than in 1996[9]) supply food and services such as landscape and biodiversity preservation. Farms interact with other farms, suppliers, buyers, controllers, regulators, professional or label organizations, research, schools, and extension services, IT and other service providers, and cooperatives. Public administrations supervise the implementation of regulation. Some private organizations execute specific regulatory tasks under public supervision (*e.g.*, the operation of the national animal control database, BDTA, by *Identitas* – see below). All these actors use digital systems. Farmers supply information about their farm to service providers and other organizations. Information concerning *e.g.*, prices, revenues, livestock health, or crop productivity can be sensitive for the farmer and is provided under contract or license agreement. In return receivers of the information provide subsidies, premiums, or other services based on the data they process. Each organization digitizes the information it gets and records it in a database that it operates. Data management comes at a cost for organisations, so the data they collect is tailored to fit their needs. It is redundant, and can be inconsistent, among these independent systems. Redundancies in turn come at a cost in data management for

7 Tiwana *et al.*, 'Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics' (2010) ISR Vol 21.

8 <www.bfs.admin.ch/bfs/en/home/news/whats-new.assetdetail.24605850.html> as of 31 May 2023.

9 Sandoz (1999), ibid.

farmers. Some organizations control the data they receive for accuracy, and errors can carry the *risk* of penalties for farmers.

Since the late 1800s, the collection of data on farms had mainly been done by the Union of Swiss Farmers, which used it for statistical, extension, and political purposes. As long as pen and paper were the backbone of information management, the effort required to collect and manage data refrained institutional actors in the sector from developing market or management practices in agriculture that would require the collection of detailed information on farms. Within a few years-time, database technologies, personal computers, and web-based applications made it possible for public administrations and private organisations to collect information directly from every farm and extract value out of large amounts of digital data. But at the other end of the process, *i.e.*, at the source of the data, the farmers could not follow up. The information infrastructure of agriculture had become a mille-feuille of institutional platforms, some loosely connected through APIs, some standing alone, each with their own clientele and caring primarily for their own needs. The multitude, heterogeneity, and complexity of data requirements from too many actors resulted in administrative burden, risks, and a growing dissatisfaction.[10] The deployment of information technologies since the mid-1990s had led by the early 2010s to a *reverse salient*, a situation where change is hindered by practices which, for some reason, prevent innovation.[11] [12] At least the situation was presented in that way by a consortium of private actors, indirectly supported by political interests close to the economy, who proposed to build a *unique* (*centralized*) *database* for the management of *all the data in the sector*. Unicity was the main argument in favour of the proposal and centralization was presented implicitly as a consequence. The database would be complemented with smart-farming *modules*. The resulting platform promised to be a simple means to solve the data problem and to lead farmers into a new age of digital profitability. The Barto project was born.

10 Droz *et al.*, *Malaise en agriculture. Une approche interdisciplinaire des politiques agricoles France-Québec-Suisse* (Karthala Editions 2014); Stiefel, 'Les données du problème. Une plateforme numérique inadaptée à l'agriculture suisse' (2022) Etudes Rurales, 209.

11 Hughes, 'The evolution of large technological systems' (1987) in Bijker, Hughes, & Pinch (eds) *The social construction of technological systems* MIT Press, 51.

12 Slota & Bowker, 'How infrastructures matter' (2017) in Felt, Fouche, Miller, & Smith-Doerr (eds.) *The handbook of science and technology studies*, MIT Press.

Many farmers, administrations, and private organizations however agreed neither to the proposed centralization of ("*their*") data nor with the ensuing private control of all of the sector's data by a self-promoted benefactor.[13] This led to the counter-initiative called ADA to develop a solution to data-sharing that could be used to relieve the pressure on farmers *and* to curtail the deployment of Barto. It was supported by organizations in the integrated, organic, and plant production sectors and represented 50% of Swiss farmers.

C. Definitions and conceptual framework

We explore *dVAT* in this socio-technical context from the perspectives of 1) farmers who supply sensitive information to organisations that make some usage of the corresponding data in their digital information systems, possibly returning a tangible benefit to the originator of the data (*e.g.*, a subsidy, a premium, or market access for their product); and of 2) the abovementioned organisations when their digital systems exchange sensitive data.

Farmers and organisations belong to the *analogical* world. We need to be able to qualify the notions above in that context (exchange of *information* to obtain/deliver tangible benefits) in order to understand how they can be declined in the digital context (production, exchange, and usage of *digital data* for the computation and traceability of the benefit). To study *trust* in this context, we use the ABI framework. Although agriculture is evidently not an enterprise, nor an organization in the classical sense, its organizational characteristics justify the framework which was designed initially in the context of organization studies.

The definition of trust proposed by Mayer, Davis and Schoorman is "the willingness of a party to be *vulnerable* to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the *ability to monitor or control* that other party". [14] This abundantly referenced definition (the paper has been cited over 30'000 times) also encompasses both the notions of vulnerability and of accountability. The model has been used to study trust in contexts

13 Stiefel (2022), ibid.
14 Mayer *et al.*, ibid.

that go beyond organizations.[15] [16] [17] We use it here to study vulnerability, accountability, and trust in the digital context.

Mayer *et al.*, emphasize the *risk* that a trustor is willing to take in order to benefit from the outcome of an action executed by a trustee whom the former potentially does not *control*. *Ability*, assessed by the trustor, refers to the capacity of the trustee to execute precisely that action, independently of any other actions the latter might or might not be able to undertake. *Benevolence* is the belief by trustors that trustees are not acting on their own profit-driven motives, but genuinely want the trustor's good.[18] *Integrity* is how much the trustor perceives that the trustee is attached to principles that the former finds acceptable. Based on their review of the literature on trust, Mayer *et al*. select these three factors to represent what trustors might generally *take into account* when evaluating the risk of an action that they have trusted another party to execute.

Relatively to data sharing, we consider vulnerabilities, risks, and benefits between farmers and organisations, and between organisations. We start from a situation where: 1) farmers have a relationship with selected organisations whom they provide sensitive information to. A contract or a software license agreement exist between the parties and regulate the production and the usage of the corresponding data, as well as the possibility to transmit the data to third parties. Organisations are accountable to farmers under the provisions of these private or public contracts; and 2) organisations are autonomous entities that operate under legal constraints. They are liable for their actions under their own responsibility. Specific contracts *between organisations* concerning the exchange of data might exist. In this case, *both* entities must conform to regulation on the access to sensitive data of third parties.

At this point Barto and ADA come into the picture. Neither one aims at changing the relationship between farmers and organisations as described in 1) and 2). However, they strongly modify the reasons, the way, and the means by which data are to be shared in agriculture. Do *new* vulnerabilities,

15 Ward *et al.*, 'Trust building and the European Reference Network for Critical Infrastructure Protection community' (2014) IJCIP Vol 7, 193.

16 Bodó, 'Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators' (2021) *New Media & Society* Vol *23*, 2668.

17 Sasse & Kirlappos, 'Design for Trusted and Trustworthy Services: Why We Must Do Better' (2014) in *Trust, Computing, and Society* CUP, Part 3, 229.

18 Hardin, R., *Trust and trustworthiness* (RSF 2002).

risks, and benefits emerge from these projects? Might *old* vulnerabilities, risks, and benefits be altered by them?

Farmers, students, and patients are physical *persons*. They use *computer systems* (mobile devices, laptops, personal computers) in their daily activities. Some of these digital systems might be large, or seem to be, like the computer system that operates a modern farm. But they are small relatively to the information *systems* of private or public organizations like the ones we consider in this paper. Those systems are operated by professional IT staff. They are built and maintained according to strategies and guidelines that relate to the discipline of *enterprise architecture*.[19] They support complex functionalities at the core of an organization's business. They comprise databases and applications, run on private networks, and their connexion to the Internet is very sensitive. They might have evolved over long periods of time and parts of this infrastructure might be *legacy*, which means, basically, outdated but too important to throw out and too expensive to adapt. Some functional components (*e.g.*, enterprise resource planning, ERP) might be licensed from third party software providers and operated remotely *out of the cloud*. These large enterprise *information systems* are owned and controlled by organisations under their individual legal responsibility, and for their own profit if the owner is a private actor.

People and organizations *interact*. When digital systems mediate interactions, those systems *interoperate*. Interoperability is a coordinated exchange of data between systems over a digital *platform*. At the lowest level the platform is TCP/IP. At higher levels it might be *e.g.*, FTP, HTTP, a webservice or e-mail, Amazon, Facebook, or Uber, or SWIFT.[20]

We use a definition of "software-based platform" to anchor the notion of *platform*: "the extensible codebase of a software-based system that provides *core functionality shared* by the modules that interoperate with it and the interfaces through which they interoperate".[21] The terms "core", "shared", and "functionality", will come back into focus when we discuss trust in relation to platforms. Most platforms considered in the literature are *centrally controlled and proprietary*.[22] Although it is more restrictive than the

19 Ross *et al.*, *Enterprise Architecture as Strategy. Creating a Foundation for Business Execution* (HBS Press 2006).

20 Scott & Zachariadis, 'Origins and development of SWIFT, 1973–2009' (2012) *BH* Vol *54*, 462

21 Tiwana *et al.*, ibid.

22 Hanseth & Bygstad, ibid.

definition, this is actually the model considered in the research note on platform evolution.[23] It also applies to large social media. This type of configuration tends to be problematic, as the literature has shown for platforms like Twitter or Facebook.[24] *Service* platforms like the latter or like Barto are controlled by their owner over application programming interfaces (APIs) that give access to functionality and data shared by the system. The sharing of functionality goes from the core (the platform owner's information system) to the periphery (modules) and the sharing of data basically goes in the other direction.

However, digital platforms in the sense of the definition need not be centrally controlled nor proprietary. *Interoperability* platforms like in particular, TCP/IP, FTP, and HTTP are not, and neither was ADA by design. These different characteristics of platforms are described in and are relevant to understand platform trustworthiness.[25]

D. Methods and materials

Our appreciation of Barto relies on the fieldwork of the first author.[26] Interviews were conducted between January 2018 and September 2019 with *ca.* 40 actors in the sector. These included farmers (5) and representatives of agricultural organizations: agents of public administrations (11) and of professional defence (2), representatives of control bodies (6), certification bodies (2), professional associations and companies in the animal and dairy sectors (6), IT service providers for agriculture (4), and system operators of these same organizations (7). Interviews were recorded, transcribed, and coded using Nvivo. Section 5 gives a summary of this work in relation to our concerns here.

---

23 Tiwana *et al.*, ibid.

24 Bucher, 'Objects of intense feeling: The case of the Twitter API' (2013) Issue 3 *Computational Culture* <http://computationalculture.net/objects-of-intense-feeling-the-case-of-the-twitter-api/> accessed 5 June 2024; Puschmann, 'The politics of Twitter data' (2013) *HIIG Discussion Paper Series*; Helmond, 'The platformization of the web: making web data platform ready' (2015) *Social Media+Society*.

25 Sandoz & Stiefel, 'Untying the knot between software-based platforms and information infrastructures' (2022) <www.researchgate.net/publication/363582508> accessed 5 June 2024.

26 Stiefel (2022), ibid.

In parallel, the second author held meetings in ADA with over 50 representatives of public and private organizations, and with farmers and researchers, covering in particular the German-speaking part of Switzerland, that he reported back to the ethnographer who held a field diary on ADA (725 pages and 223 entries). The details are presented in her thesis.[27]

The appreciation of ADA is rooted in conceptual considerations. It was designed in view of stopping Barto by proving that data-centralization, if at all possible, was not necessary to solve the reverse salient in data management to the satisfaction of the actors in place. The approach explicitly left the choice to organisations whether or not to participate. The design would rely on a model of *actors exchanging information* over their information systems (*e.g.*, where notions such as liberty of association, autonomy, or trust apply), and not only of technical systems that interoperate over APIs.

E. Case studies

During 2018 and 2019, interviews revealed a range of concerns and risks of organizations and farmers regarding data management by Barto. Data-owners (farmers) and representatives of data-users (organizations) were concerned by the project's stakeholders, by the dependencies the system would create, and by the possible consequences. We start by describing how data is used by farmers and organisations, before reporting on their respective concerns.

Farmers use digital systems in *production* and in *management*. In *production*, systems are used for *functionality* (*e.g.*, to control the gate to an automatic milking machine, depending on how long a cow has been feeding) and for *decision-support* (*e.g.*, to suggest when to irrigate or to treat a crop, depending on environmental factors). Systems use data that is generated locally (*e.g.*, by machines, sensors, robots) or remotely (*e.g.*, by weather stations or global navigation satellite systems). These systems produce new data. They are developed by the agroindustry which supplies machines and inputs. Suppliers usually keep under tight control the data that their systems produce and use.

In *management*, digital systems are used for *resource planning*. For this type of system, data is related to resources, to products, to the market, and

27 Stiefel Léa, *Politiques des architectures numériques. Cheminements ethnographiques dans la conception d'alternatives à la centralisation des données* (University of Lausanne 2023).

to financial, regulatory, or other factors. Farmers themselves supply some of the data used for resource planning, *e.g.*, dates and places of sowing, types of crops or treatment, produce and income, costs, etc. The rest of the data is supplied or sourced by the software provider who develops, operates, and maintains the system.

Increasingly, data used and produced by these systems is stored in remote databases operated by their service providers. The latter compete to increase the number of farms that use their software, which collects, computes, and accumulates data. Data can be used to improve a system, but it can also be a valuable source of information on the market. So, data is precious to service providers. It is also sensitive for farmers, because it describes quantities, quality and maturity of products, customers, costs and prices, as well as modes of production that can be strictly contracted or regulated.

The evolution of digital technology *as a service* has brought advantages to farmers as it often simplifies management, and enhances the quality and availability of information. It has also benefited database operators by giving them free access to large quantities of valuable data (all the while enabling the cost of software maintenance and of customer relationship management to decrease).

Organizations use data to manage information on individual farms and transversally through the sector depending on their mission. Public administrations supervise the implementation of regulation, notably of subsidies; producers organizations define requirements for labels (*e.g.*, organic, integrated, traditional, etc.) and distribute individual quotas, which, if both are respected by the farmer, bring a premium on the market; professional organizations compute statistics to define their policies and lobbying strategies; some private organizations are supported by the regulator, *e.g.*, to prevent inbreeding in livestock by controlling the distribution of genes to farms and to improve breeds by increasing the resistance of animals to pathogens; etc. All of these activities require sensitive data from farmers who must deliver if they want a shot at the benefits. For each organisation, its data is homogeneous and might have a broader coverage than the market share of any service provider (see above). Organizations store the data in their own database and develop in depth knowledge, both transversal and specific to individual farms, on sensitive questions.

To summarize: data concerning farms is maintained in dispersed databases operated by independent organizations, *i.e.*, data-*users*. Each organization defines procedures (*i.e.*, in particular *when* the data is collected)

and data formats (*i.e.*, how information is digitized) according to its needs. To prevent sanctions and other negative consequences of false interpretations, farmers (*i.e.*, the data-*owners*) need to control what information goes where, when and in what form.

I. Barto: a service platform on top of a centralized database

Project Barto proposed to collect all farm data in a unique central database and, on this basis, to develop smart services for farms (decision support modules). Farmers explained their concerns to the ethnographer:

- among the project's stakeholders were the largest agricultural cooperative in Switzerland *Fenaco*, both the main supplier and a major buyer of products for farms; a European software development company *365-FarmNet*, linked to the cooperative by a German machinery manufacturer *Claas*; and two important publicly owned, *resp.* supported, Swiss organizations *Identitas* and *Agridea*. Farmers were concerned that the project was backed by a conglomerate of powerful private players. The centralized database would be able to provide full visibility into what was happening on all farms, on a daily basis. Combined with their own private decision-support tools, the database would enable the cooperative and its foreign partners to drive the demand for inputs and the supply of agricultural products, and to influence market and supply prices. Farmers perceived a high risk of "vertical integration", bringing commercial vulnerability because a third party would control all their data. Meanwhile they would retain the burdens of debt and production risks (such as losses due to weather or disease). They would *pay* to use "services" developed on the basis of *their* data and would be held *liable* by contract for its quality, while all the profits would go to the database owners;
- it was unclear how data would flow between organisations associated with the centralized database. Without control over the flow of their data, they were at risk. For example, if data inadvertently reached a government agency, indicating high nitrogen levels in one field, the farm could lose subsidies, even if they were compensated in another (which happens daily on many farms). If data from a government inspection showing a health problem of an animal was inadvertently passed on to a dealer, the farm and its neighbours could be side-lined (what actually

happened to an entire village because of a single sick animal) for fear that disease might spread from a shipment to the slaughterhouse;

Barto also proposed to redistribute the data out of its central database to data-users (*i.e.*, organizations) according to their needs. For the latter, centralization also posed problems:

- organizations would have to "log in" to the central database to access the data they needed and that had been previously supplied to them directly by the farmers. There was no guarantee that they would actually be allowed to access the data in contents and formats, and at times necessary to carry out their duties, nor was there any indication of the price to be paid. Centralization promised to jeopardize the autonomy of the organizations, to the point of threatening their very existence;
- project Barto planned to store farm data in a cloud in Germany[28], under the control of its software partner. This posed a problem of data sovereignty, which was unacceptable to public administrations. It also posed problems as to how to resolve conflicts between farmers and organizations arising from data management, with data residing in the legal realm of a foreign authority;
- the centralized database would introduce a distortion of competition: faced with foreign stakeholders who would concentrate all the farmers' data, small Swiss organizations, e.g., high quality local insemination cooperatives, would not stand a chance to compete and were at risk to disappear;
- Barto promised that organizations could propose functional modules connected to the central database, but it was not clear to organizations if this openness would be observed in reality beyond the rhetoric. Its owners could act single-handedly, as long as they controlled the platform's APIs and the data.

II. ADA: a peer-to-peer platform for authorized data transmission

ADA emerged in reaction to Barto and to the problems and threats that were perceived by the sector's actors. The opposition between the two

28 Swissmilk, <https://api.swissmilk.ch/wp-content/uploads/2019/06/praesentationen-vorstellung-ada-barto-hotel-bern-2018-02-28-de-fr.pdf> accessed 5 June 2024.

projects is clearly assumed in this paper and was public.[29] Our purpose is not Manichean: ADA was not a commercial competitor, nor was the project an attempt to *take over* the information infrastructure of Swiss agriculture. ADA's *proposed* alternative to Barto's approach was to provide a transversal component in agriculture, that farmers and organisations could freely use to improve data management where it was meaningful, and possibly reduce costs, inconsistencies, and redundancies. The section describes the rationale and functioning of ADA. It does not intend to be rightful or prove correctness, but rather to show the complexity of sensitive data sharing and to sketch its technical limits by connecting the concerns of the actors with the constraints, design features, and technical mechanisms that were embedded in ADA. The proposition consisted in providing the digital ecosystem of agriculture with a means 1) to authorize and trace the exchange of sensitive data between the information systems of data-users 2) without altering the practices (of actors) or the operations (of systems) in place. The technical solution would be a peer-to-peer platform where the peers would be organizations, each operating a *node* of the platform to which it would connect its information system over an API that it controlled alone. The platform, composed at any time of all the operational nodes, would be neither proprietary nor centrally controlled. Its only (core shared) functionalities would be:

a) for the data owner (*i.e.*, the farmer) to grant and manage authorizations; and
b) for the data users (*i.e.*, the organizations that operated sensitive data) to exchange data if the authorization had been granted by the owner, and if and when both users agreed to do so.

Nodes would manage and make data persistent only when it was related to these two functionalities and only when their peer was directly concerned. Sensitive data of farmers would be sent and received by nodes, in order to be stored and accessed in their respective systems, only by the users of that data, under the separate contracts or software licenses they had previously established with the data owner (see section 3), and on the respective system. Transmission would be bilateral and direct between the two nodes of the peers concerned. Authorization would be tripartite. How a data-owner was identified by a data-user would not be shared (the contrary

29 Swissmilk, ibid.

would imply a dependency between operators and violate the principle of autonomy). Traces necessary for a peer to positively prove *correct* behaviour would be stored locally in its node after each sensitive operation and kept under the control of that peer only. Traces might be *removed* from a node by its peer, because of the latter's full local control over its node. So, there could be *no proof of misconduct*, only *an absence of proof of correct behaviour*, that could lead to the suspicion of a rule violation. These considerations follow the technical line of what is possible or not in an asynchronous (general) distributed system. They determine the scope and the limits of accountability for data sharing between organizations. The platform would be *fully* distributed. All roles would be *symmetrical* (what a peer could, every peer could, with the same constraints). Within its scope, the platform's architecture would preserve the autonomy of each peer and guarantee the freedom of association, an equal treatment, and symmetry among peers.[30]

Technically, the project faced two challenges: *i*) *asynchrony* in distributed systems (which is usually overcome by using the master-slave paradigm underlying internet protocols based on APIs controlled by the master); and *ii*) *matching the different meanings attributed to information* by a sender, a receiver, and a farmer *using digital data* (which is usually overcome by using data standards and fixed formats agreed by or imposed to data-users).[31] Problem *i)* is inherent to communication in distributed systems and requires its own toolset to be correctly mastered, notably to maintain shared states in asynchronous configurations. Problem *ii)* is trickier and is usually solved by using data standardization, an invasive mechanism that can provoke side effects.[32] It would imply a change in system processes and organization practices, neither of which was acceptable for ADA's sponsors. A mechanism called *segmentation* was designed to bridge the gaps in time and meaning that could arise between organizations that would exchange data over ADA. The same mechanism underlay the touch-screen app used by farmers to manage authorizations. Organizations would know how to associate information that they managed for farmers to digital data using segmentation. So, organisations whom farmers trusted (*i.e.*, *from* which they accepted to *send their data* to other organisations) could help them

30 Stiefel & Sandoz, 'Une plateforme en pair-à-pair pour l'échange de données: l'émergence d'un commun numérique' (2021) *Terminal.*

31 Hardstone *et al.*, 'Standardization, trust, and dependability' in *Trust in Technology: A Socio-Technical Perspective* (Springer 2006).

32 Hanseth *et al.*, ibid.

manage authorizations by providing guidelines and templates (see the discussion below).

The platform was designed as a permissioned, fully distributed and symmetrical network of identical nodes, each operated under the control of one peer. The node was designed as a structured set of *services*, organized in functional layers as in the OSI model of ISO.[33] Each service *instance* in one node *logically* interoperated only with the instances of the same service of other nodes.[34] The platform's technical architecture, its node implementation, and the connexion of legacy systems to nodes, were based on the Kubernetes (K8s) microservice architecture. The gRPC standard interface framework (for APIs) and the Hyperledger Fabric distributed ledger (for the publication of source datatypes and usages) were available at the time of the project on top of K8s. All three technologies were standalone and freely available in open-source code.

F. Discussion

In the previous sections, we examined the two projects that aimed at solving a digital reverse salient caused by uncontrolled digitization *following* a structural transformation in Swiss agriculture, that was *independent* of digitization.

Barto was a service platform with a centralized database and APIs controlled by the platform owner. It proposed to manage all of the farm data in the sector. Its stakeholders were a consortium of private actors with commercial interests in the agri-food sector. These interests could leverage Barto by concentrating exhaustive vertical and transversal information in one system they would control. The business model was a service platform with complementors, like Facebook.[35] Complementors would supply smart-farming modules. Organisations would delegate data management to the platform and access the data they needed over its APIs. The project was capital intensive (over 10MCHF in 5 years), and technically and commercially risky. Feasibility was only sporadically questioned though it represented a significant risk: if the project could not collect all the data or

33 ISO/IEC 'Information technology — Open Systems Interconnection — Basic Reference Model' (1994).

34 Sandoz, 'Inter-operating Co-opeting Entities: A Peer-to-Peer Approach to Cooperation between Competitors' (2020).

35 Helmond, ibid.

implement all the functionalities required, the platform would become just another farm-ERP, possibly with privileged relationships along the business lines represented by specific stakeholders. Development was conducted internally by one of the stakeholders.

ADA was a peer-to-peer platform composed of an evolving and open number of nodes connected each to the information system of one organisation (a peer). The APIs and the services of the platform were distributed in the nodes, each node being technically and legally controlled by the peer it serviced. ADA itself did not manage nor store any data. Farm data remained in operators' databases. The project's stakeholders were associations of farmers and professional organisations. Its business model was collective funding of the initial instance and free open-source community development and maintenance once the platform would be in production. Access was free for farmers and auto-financed by organisations according to their needs. Organisations would continue to operate their own information system infrastructure, legacy systems, and databases, and operate their own node. Farmers would be implicated in data management through the authorisation function for data exchange between operators. The main motivation of stakeholders was to curtail Barto which was seen as an existential threat. Technical *dependability* of the platform was a design goal, but it was never discussed *in detail* with ADA's sponsors. The initial version of the platform cost under 1MCHF. The project was commissioned by the organisations and development was external.

The opposition between the two projects along clear functional, organizational, and architectural lines is an opportunity to study the potential and limits of digital technologies in relation to *dVAT*. Before Barto and ADA were launched, farmers' data were distributed throughout a landscape of organisations, each operating its database and accountable under its own technical and legal responsibility: *dVAT* were point to point (farmer to organisation) and determined by contracts. The *data-for-service* relationship was biased in favour of the organisations and created asymmetric dependencies, but the farmers could quit in most cases, exceptions being the enforcement of regulation (like animal control). With Barto, this freedom would be lost, creating a new type of digital vulnerability for farmers: complete visibility, and the economic threat of verticalization. Additionally, every organisation but one (Barto) would become vulnerable to the whims of the latter.

With ADA, the relationship between farmers and organisations remained unchanged. Farmers were provided with a means to control and trace eventual data-flows between organisations, making them less vulnerable to data-leaks through undisclosed back channels. Consequently, the accountability of organisations would be reinforced and trust of the farmers towards organisations would follow where accountability, and hence trustworthiness, could be established. Where this was not the case, the farmer retained the possibility to quit, as previously. With Barto, trust fell out of the equation: the farmer would not *willingly* take a risk (of entrusting their data to the consortium), but would be compelled to do so. Additionally, farmers would be made accountable for errors, not the contrary. For organisations, Barto became a new intermediary cast between them and the farmers. Not only would organizations become vulnerable towards the central actor, as described above, but technically, the centralized platform and API configuration would impair their ability to fulfil their missions.[36] They would remain accountable to farmers for the quality and the timeliness of their services, but would no longer be able to control what they delivered and when. With ADA, each organisation controlled, operated, and was responsible for its own node, preserving accountability to farmers. Mutual liabilities between organisations concerning the transmission of data over ADA would have to be defined, either collectively or bilaterally.[37]

The two approaches were technically different (centralization *vs.* distribution) and the choice of the approach had heavy consequences on the vulnerability of actors, on their accountability, and on their mutual trust relationships.

G. Conclusions

As opposed to platforms with millions or tens of millions of users worldwide like Facebook or Amazaon, in this paper we explored the topic of digital vulnerability, accountability, and trust (*dVAT*) *in the small*, *i.e.*, the design of sensitive data sharing in a small economic sector in a small European country, with homogeneous legislation. A few tens of thousands of persons (farmers) must make decisions concerning which organizations

36 Stiefel & Sandoz, 'Critique de la concentration: une analyse des relations de dépendance sur les plateformes numériques' (2022) *AIMS Conference on Strategic Management.*

37 Stiefel & Sandoz, 2021, ibid.

they can or cannot entrust their sensitive data with. A few hundreds of organizations, private or public, who structure the activities of the sector, traditionally consider the data they use as "*their*" own property. How can accountability and trust be sown into this type of environment? When Barto threatened to take over data management in the sector, ADA attempted to give some control over their data back to farmers. The project designed a peer-to-peer software-based platform that had a key characteristic: it was not controlled (neither owned, nor operated) by a single actor or a small group of actors who might aim to leverage data to sustain their interests. It was operated by *every* actor, within their circle of control and legal responsibility, and worked symmetrically relatively to all the participants.

The platform sent the question of accountability and trustworthiness back to each organization that managed sensitive data of farmers. The farmer could privilege a trusted relationship with one player or another, or delegate the assessment of platform usage to several independently. In this decartelized configuration, the agency of the farmer would encourage trustees to be more accountable.

The peer-to-peer platform was designed to address the concerns of data owners and of data users, and to enhance accountability and mutual trust based on its socio-technical architecture.[38] Farmers demand privacy from the organizations that manage their data. They *trust* them more or less to provide services in accordance with the information they supply about their farms (aptitude). They do not always trust them to use the data to their sole benefit (benevolence). They are sometimes at risk that the data will not be used properly (integrity). An architecture that relies on transparency in how data is collected, circulated, and used by operators could reduce vulnerabilities, strengthen accountability, and enhance trust. In a framework with clearly defined rules, control mechanisms and sanctions, that the user community itself could steer according to changing conditions and needs, possibly under the guidance of external authorities[39], farmers (and organizations) might better accept, and even push for, data sharing. Data management might then become less complex and more efficient, and the digital vulnerability of data-owners might be reduced.

38 Mazzella *et al*., 'How digital trust powers the sharing economy' (2017) IESE Insight, Issue 30, 24.

39 Hess, C. & Ostrom, E. *Understanding Knowledge as a Commons. From Theory to Practice* (MIT Press 2007).

CONCLUSIONS

Digital Vulnerability in European Private Law – Conclusions

Reiner Schulze

A. Introduction

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

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

B. A new challenge for European Private Law

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L 277/1 (Digital Services Act - DSA), art 1 para 1.

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

17 Schulze (n. 2 above) 145.

18 See n. 3 above.

C. Concept and cross-cutting nature of digital vulnerability

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

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

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

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

21 Fundamentally, see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (General Data Protection Regulation - GDPR).

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

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

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

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

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

24 See n. 21 above.

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

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

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

25 See n. 16 above.

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

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

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

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

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

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

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

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

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

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

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

D. Some approaches for legal responses to digital vulnerability

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

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

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

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

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

36 Schulze (n. 2 above) 159ff.

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

I. The multilevel dimension

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

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

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

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

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

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

38 N. 21 above.

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

40 N. 15 above.

41 N. 22 above.

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

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

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

II. Interaction with public law

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

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

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

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

III. Consumer protection and protection of Internet users

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

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

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

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

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

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

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

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

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

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

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

E. Further tasks for legislation and research

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

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

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

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

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

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

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

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