ANA S. G. PEREIRA
8989

DECEPTIVE DESIGN PATTERNS UNDER EU LEGISLATION AND VULNERABLE DATA SUBJECTS' PERSONAL DATA:

Impact On User Autonomy and Ability to Consent

Dissertation to obtain a Master's Degree in Law, in the specialty of Law of Social Innovation.

Supervisor:
Professor Dr. Graça Canto Moniz, Professor of the NOVA School of Law

September 2024

ANA S. G. PEREIRA
8989

DECEPTIVE DESIGN PATTERNS UNDER EU LEGISLATION AND VULNERABLE DATA SUBJECTS' PERSONAL DATA:

Impact On User Autonomy and Ability to Consent

Dissertation to obtain a Master's Degree in Law, in the specialty of Law of Social Innovation

Supervisor:

Professor Dr. Graça Canto Moniz, Professor of the NOVA School of Law

September 2024

ANTI-PLAGIARISM STATEMENT

I hereby declare that the work I present is my own work and that all my citations are correctly acknowledged. I am aware that the use of unacknowledged and extraneous materials and sources constitutes a serious ethical and disciplinary offence.

Ana Sofia Gregório Pereira (Student No. 8989)
September 2024

Para a minha avó,
Que sempre quis que sonhasse mais alto que o céu.

DEDICATION AND ACKNOWLEDGMENTS

A dissertation cannot be written on its own – whoever says otherwise is either lying or has gone mad in the process. This entire thesis would not be possible were it not for the unyielding support (and faith) those who are the closest to me showed me all throughout this process.

First, I would like to thank my family for always believing in me, and for inspiring me to always aim higher. To my uncle Carlos and my aunt Catarina, for always being my inspirations and my role models, and for the quintessential support they have always shown me, especially during this chapter of my life. To my uncle António and to my aunt Alexandra, for their always kind words. To my uncle Pedro and my aunt Vera, for always being so close and so worried, despite the distance. To my mother, Paula, who taught me to fight from an early age, and to my brother Jaime, for being my greatest friend, always. To my grandfather, José, for teaching me what it means to work towards our goals and to my late grandmother, Maria José to whom this dissertation is entirely dedicated, for showing me the meaning of true love and perseverance. A huge "thank you", the size of the world, to Maria Emília and Oswaldo, to Hélio and to Lidório, for all the support and faith in this project, and in my person.

To Gonçalo, for always being by my side, through thick and thin, and for not allowing me to shut myself away from the rest of the world, or from doubting myself. For being my light, and the arms around me when I could not bear to read not even one more word from another article without despairing. There are no words to express how grateful I am for you.

To my dearest friends, who never let me down, not even for a single second, throughout this dissertation and through life itself, Sara, Madalena, Mariana, Beatriz, Soraia, Catarina (Coelho), as well as Vanessa, Iolanda, Catarina (do Vale). You have taught me the meaning of true friendship, and I would have not made any of this without you. You made this process so much lighter, so much more bearable, and you are all a very special part of my life. A special thanks to Madalena, to Catarina Coelho and to Iolanda, who read the first draft of this dissertation and whose comments were incredibly useful to improve it.

To the friends who I made during my masters' degree at NOVA, Yuliya, Catarina, Joana, Mafalda and Anna, thank you for your support, always.

To all my friends at Box Caramela, and especially to Pedro, Maria Inês, João, Catarina, Francisco, João, Nicolas, and Ricardo, thank you for always encouraging me to push through, and for being so positive, always (especially when I was not).

I would like to thank my supervisor, Professor Dr. Graça Canto Moniz, for the guidance and support showed through this dissertation, and to NOVA School of Law, the faculty which became my home for the last two years. This dissertation also would not be possible without the funding from Fundação José Neves' ISA, so I would also like to show them, and their staff, my gratitude.

A very special thanks, as well, to my colleagues at ARAC, for all of the support during this phase, especially to Alzira, Maria and Sandra, for putting up with my never-ending stress.

Last but not least, I must thank Dr. Harry Brignull, who not only took the time to meet with me to discuss the topic of this dissertation, but who also offered to send me an Advanced Review Copy of his book, which was crucial to this work.

To everyone, thank you so much. You make life so much more colorful, and I am grateful for each and every one of you.

QUOTING AND OTHER CONVENTIONS

For the present dissertation, we opted to cite using the American Psychology Association's style (APA, 7th edition), on footnotes.

LIST OF ABBREVIATIONS

GDPR – General Data Protection Regulation

EDPB – European Data Protection Board

WP29 – Working Group on Article 29

EU – European Union

US – United States

DSA – Digital Services Act

UI – User Interface

UX – User Experience

ICD – International Council of Design

CNIL - *Commission nationale de l'informatique et des libertés* (French Data Protection Authority)

ECHR – European Court of Human Rights

TFUE – Treaty of Functioning of the European Union

UCPD – Unfair Commercial Practices Directive

DPIA (Data Protection Impact Assessment)

DMA (Digital Markets Act)

CJUE – Court of Justice of the European Union)

FTC – Federal Trade Commission

ECOA – Equal Credit Opportunity Act

COPPA – Children's Online Privacy Protection Act

ROSCA – Restore Online Shopper's Confidence Act

CAN SPAM – Controlling the Assault of Non-Solicited Pornography and Marketing Act

TSR – Telemarketing Sales Rule

TLA – Truth in Lending Act

CPRA – California Privacy Rights Act

CPA – Colorado Privacy Act

CTDPA – Connecticut Data Privacy Act

OCPA – Oregon Consumer Privacy Act

NY GBL – New York General Business Law

UCPA – Utah Consumer Privacy Act

MCPA – Massachusetts Consumer Protection Act

WCPA – Washington Consumer Protection Act

VCDPA – Virgina Consumer Data Protection Act

DTPA – Texas Deceptive Trade Practices – Consumer Protection Act

DETOUR Act – Deceptive Experiences to Online Users Reduction Act

GM – General Motors LLC

VLOP – Very Large Online Platform

DPA – Data Protection Authority

DECLARATION

O corpo da presente dissertação, incluindo espaços e notas, ocupa um total de 195 173 caracteres.

The body of the present dissertation, including spaces and notes, occupies a total of 195 173 characters.

ABSTRACT

The topic we propose to investigate throughout our dissertation is the impact of deceptive patterns, particularly, on vulnerable users' consent and autonomy.

Deceptive patterns are tactics employed by companies to purposefully confuse users and lead them to make choices they would not to the benefit of the companies running the platform.

Consent (and personal data) obtained via the usage of deceptive patterns cannot be valid, for it is obtained illegitimately, in violation of the structuring principles of fairness, transparency, data minimization, and data protection by design and by default. In particular, towards vulnerable users, the usage of these tactics can prove itself to be quite problematic for not only is these users' ability to consent hindered from the start, from a social point of view, it is dangerous and can materialize in economic, emotional, and physical damages.

Regulation is urgent, but not sufficient. When the digital economy gallops, the EU legislator, as well as all relevant stakeholders, must fly at the speed of light to catch up and protect the public interest behind this problematic.

Keywords: Deceptive patterns, vulnerability, data protection, privacy law

RESUMO

O tema que nos propomos investigar ao longo da nossa dissertação é o impacto dos *deceptive patterns*, em particular no consentimento e na autonomia dos utilizadores vulneráveis.

Deceptive patterns são táticas utilizadas pelas empresas para confundir propositadamente os utilizadores e levá-los a fazer escolhas que não fariam em benefício das empresas que gerem as plataformas eletrónicas.

O consentimento (e os dados pessoais) obtido através da utilização destas táticas não pode ser válido, pois é obtido de forma ilegítima, violando os princípios estruturantes da transparência, minimização de dados e proteção de dados desde a conceção e por defeito.

Em particular, para os utilizadores vulneráveis, a utilização destas tácticas pode revelar-se bastante problemática, pois não só a capacidade de consentimento destes utilizadores é prejudicada à partida, como, do ponto de vista social, é perigosa e pode materializar-se em danos económicos, emocionais e físicos.

A regulamentação é urgente, mas não suficiente. Quando a economia digital galopa, o legislador da UE, bem como todos os intervenientes relevantes, têm de voar à velocidade da luz para recuperar o atraso e proteger o interesse público subjacente a esta problemática.

Palavras-Chave: *Deceptive Patterns*, vulnerabilidade, proteção de dados, direito da privacidade.

TABLE OF CONTENTS

Deceptive Design Patterns Under EU Legislation & Vulnerable Data Subjects' Personal Data: Impact on User Autonomy and Ability to Consent

INTRODUCTION

Attention means profit in media — that is no news. And when it comes to catching and maintaining user attention in today's digital economy, every stakeholder is an expert at keeping people — clients — glued to their screens and presenting them with content that is, apparently, perfectly matched to their desires. But is this not a double-edged sword?

On the one hand, users are rewarded by the prospect of seeing content that is more relevant and adjusted to their needs, but on the other, one must ask: how was their personal data (such as age, gender, race, academic background, professional status, etc.) obtained, and with what consent? Was it freely given and perfectly informed? All these questions keep raising concerns.

Nowadays, the competition for brain-time is higher than it has ever been, and "the methods used by those building content not only act on the attention of individuals, but also on their behavior and attention[1]". Those methods, typically employed to purposefully confuse users and lead them to make choices they would not to the benefit of the companies running the platform, such as buying more items than they intended to or disclosing more personal information than what is really necessary for processing purposes, are called deceptive design patterns (or "dark patterns", as coined back in 2009 by UI Designer, BRIGNULL, who described these patterns as "tricks used in websites and apps that make you buy or sign up for things that you didn't mean to[2]") and one of the many consequences of their usage in the construction on websites is the lack of awareness and autonomy they create in individuals regarding what they share or what they do.

With the advance of technology, user interface design and user experience design have been evolving rapidly in order to answer to a market that is ever-growing in number[3] and exigency, for they expect websites to be functional, easy to understand and customizable. So, both users and developers have been settling for ubiquitous, customized, and so-called seamless user interactions and experiences: the perfect

[1] CHATELLIER, R., DELCROIX, G. HARY, E., et al., Shaping choices in the digital world - from dark patterns to data protection: the influence of ux/ui design on user empowerment, CNIL IP Reports - Innovation and Foresight, No. 6, 2019, p. 14. Available for consultation online on: https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

[2] Brignull, H., Deceptive patterns (2010). https://www.deceptive.design

[3] According to Statista, as of July 2024, 97.5% and 96.9% are the internet penetration rates (people using the internet) of northern and western europe, respectively. Available on: https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/ (Last Access: September 2024).

interface should be highly personalized, easy to use and multimodal[4]. Naturally, these trends can be useful, for they make the user experience in digital services more convenient and simpler, two qualities that users look for when navigating the web more and more[5]. However, they can be used in a way that may influence users to act against the spirit of the General Data Protection Regulation (hereinafter, GDPR). As NORMAN highlights, "the conscious manipulation of society has severe drawbacks, not the least of which is the fact that not everyone agrees on the appropriate goals[6]".

Deceptive patterns can be defined as "practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions[7]" and one of the most concerning aspects about them is that most will go amiss or, if noticed, might be seen as marketing tactics made to generate more profit for the company using them.

The cited recital does not mention deceptive patterns but, in lieu, dark patterns. This is because, up until the final publication of the European Data Protection Board (hereinafter EDPB) Guidelines 03/2022[8], in February 2023, they were referred to as dark patterns[9]. We will use the latest designation, and therefore, whenever there is any legal, jurisprudential, or doctrinal reference to dark patterns, we will use the term deceptive patterns.

It is urgent to act against these practices, and we will look both at European and American legislation and case law so as to better understand what is already being made in the field. For years now, as we will have the chance to see, the American Courts have been ruling out several unfair practices in used by enterprises and companies[10] without referring to them as deceptive patterns. As we will have the opportunity to examine, this is slowly changing both in the United States and in the European Union, especially when it comes to the validity of obtained consent.

---

[4] Chatellier, R., Delcroix, G. Hary, E., et al., (2019) *op. cit.*, p. 9
[5] *Ibid.*
[6] Norman, D.A. (2013) The Design of Everyday Things: Revised and Expanded Edition, Basic Books, ISBN 978-0-465-00394-5, p. 291
[7] Recital 67 - 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).
[8] Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, EDPB, Adopted on February 14th, 2023, Available on: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en
[9] For comparison, see the previous version of Guidelines 03/2022: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf
[10] For instance, FTC v. AMG Capital Management (2018), FTC v. LeadClick Media (2019) and FTC v. Office Depot (2019).

First and foremost, it is important to highlight the fact that the concept of vulnerable data subject which we propose to develop and analyze does not have a proper and specific legal consecration (as opposed to the concept of vulnerable consumer). Children are the only category of vulnerable user that is precisely defined and protected. However, the recitals of the GDPR, as well as the Working Group on Article 29 (hereinafter, WP29), have been mentioning other vulnerable adults in need of protection. Furthermore, it is a concept that is still being developed by the doctrine in Europe, and thus, we will analyze this topic on the second chapter.

Secondly, the concept of deceptive design patterns is not entirely new: but the idea of regulating them is somewhat recent despite how the legal scholars have been pleading for it for a while, as we will have the opportunity to showcase throughout our dissertation.

Thirdly, to the extent of our knowledge, even though relevant legislation to regulate this issue is slowly emerging and evolving, we still consider that there still is a gap when it comes to firmly relating the usage of these practices to their impact on vulnerable individuals' decision making and autonomy, so we believe it is pertinent to look and think about this situation, in order to protect a part of population that is often rendered silent and more harmed than any other.

We are of the opinion that, given the rapid evolution of deceptive patterns, the way the legal framework has to catch up and the complexity of the topic, it is urgent to bring light and give a voice to the vulnerable users on the online world.

Therefore, the present dissertation will be organized as follow: the first chapter will focus on the concept of design, as, in order to understand what deceptive design patterns are, we believe it is useful to be acknowledged with some basic design principles and psychology, as these manipulative tactics not only distort those guiding principles, but also predate on the human brain's heuristics and cognitive biases.

The second chapter will define and develop the concept of vulnerability, so that we can define who the vulnerable data subject is, as well as highlight the several harms that the usage of deceptive design patterns can cause, and how they can have a heavier influence on these individuals.

Lastly, the third chapter will focus on the legal framework that can, eventually, tackle this issue, so as to protect the vulnerable data subject. In order to do so, we will make a brief comparative analysis between the European Union's (hereinafter, EU) and

the United State's (hereinafter, US) approach to these practices and conclude with some suggestions for the future.

DECEPTIVE DESIGN PATTERNS

Evolution of the concept

We have defined deceptive patterns as "practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions[11]", in light of the definition proposed by Recital 67 of the Digital Services Act (hereinafter, DSA) This is a fairly recent definition, and, as it has been noted by NARAYANAN et al., deceptive patterns may have only recently been brought to light to the general public, but they have been around for a long while and are the result of the usage of deceptive practices in retail, nudging in public policy, and growth hacking in design[12]. SANTOS et al. also present an interesting definition for these harmful design techniques, referring to them as "tricks that influence the online decisions of users about their purchases, their use of time and attention and the disclosure of their personal data[13]".

It is true that the scope of present dissertation is the impact of deceptive design in privacy and user autonomy and ability to consent, and it is also true that the purpose of this investigation is to give a legal insight on this problem. However, and although design (and/or human computer interaction) is not our field of practice and study, we still think that in order to truly understand what lies behind deceptive patterns, it is of utmost importance to delve a little into a couple of aspects before proceeding, namely the evolution (and *raison d´être*) for the existence and usage of these patterns in web and app design, as well as in user interface (hereinafter, UI) and user experience (hereinafter, UX) design, for the reasons highlighted on the introduction.

[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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

[12] NARAYANAN, A., MATHUR, A., CHETTY, M., & KSHIRSAGAR, M. (2020). Dark patterns: past, present, and future. ACM Queue, 18(2), 67–92. https://doi.org/10.1145/3400899.3400901 pp. 2-3

[13] SANTOS, C., MOROZOVAITE, V. and DE CONCA, S., (June 26, 2024) No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. Available at SSRN: https://ssrn.com/abstract=4877439 or http://dx.doi.org/10.2139/ssrn.4877439, p. 2

Design: definition, principles, and their subversion for deception

Definition

In this section, we will explore the several concepts that exist for design, before adopting a single definition, given the plethora of ways it can be described.

The Cambridge dictionary explains that (*to) design* is to *make or draw plans for something*[14]. From this apparently simple definition, we can infer that, in order for something to be considered a design, it must have a purpose; it must be planned for a certain context or specific goal. We can also look at the word's etymology in order to better support this idea: (to) design comes from the latin *designare, which,* in turn, comes from the junction of *de* (out) with *signum* (identifiying mark, sign). So, we can look at it as "to mark something out, to others". Afterwards, the Italian verb *disegnare* grew to mean "to intend" and "to draw". This later passed on to French (*dessiner),* and then to English, which uses the word design in all senses. As a noun, from the 1540s, design *meant to plan or outline, form a scheme,* and, by 1703, it evolved to mean *to contrive for a purpose*. The transitive sense of *drawing the outline or figure of,* particularly for a proposed work, dates to the 1630s, while thirty years later, it came to mean *plan and execute, fashion with artistic skill*. On the other hand, the intransitive sense of *doing original work in a graphic or plastic art* appeared by 1854[15].

Indeed, as EAMES, one of the most influential twentieth century designer stated in an interview, *"design is a plan for arranging elements in such a way as best to accomplish a particular purpose.*[16]*"*

The International Council of Design (hereinafter, ICD) takes such a definition to the next level and describes design as "*a discipline of study and practice focused on the interaction between a person — a 'user'— and the man-made environment, taking into account aesthetic, functional, contextual, cultural and societal considerations*[17]", which means that design not only is a planned activity that serves a specific purpose, it is also a

[14] 'design' (2024). https://dictionary.cambridge.org/dictionary/english/design.
[15] design | Etymology of design by etymonline. (n.d.). Etymonline. https://www.etymonline.com/word/design
[16] Design Q & A: Charles and Ray Eames. (n.d.). https://www.hermanmiller.com/stories/why-magazine/design-q-and-a-charles-and-ray-eames/
[17] What is design? (n.d.). International Council of Design. https://www.theicod.org/en/professional-design/what-is-design/what-is-design

relational concept, as one of its key elements is communication between two parties. To design is also to communicate, effectively, an idea or concept[18].

Design is also a subject in permanent evolution according to necessity - RODGERS and BREMMER have been arguing precisely that the discipline of design is in expansion since the 1950's, and that the same boundaries which once served to separate several design disciplines (graphic, textile, product, etc.) are not only becoming harder and harder to disclose, but also that it is expanding to other fields such as engineering and business[19] [20].

If at its core design used to be a tool to do no more than giving an improved look to things which would *"otherwise remain too clumsy, too severe or too bared if it were left to its naked function*[21]*",* with the evolution of times it became clear that it had a pivotal role in dictating the way people – or users – interacted with objects and with the world around them[22].

As BRIGNULL notes, nowadays, design goes way beyond arranging the way things look and *it is more about persuading and influencing people*[23]*, "tracking, testing, psychology, behavioural economics, statistics and empirical scientific research*[24]*".* This confirms yet another characteristic of design: its fluidity and mutability[25], which the cited authors call *alterplinarity* (*alternative disciplinarity)* to refer to the current state of design as a "*fluid, evolving muddle of practice that regular cross, exceed, and alter historical disciplinary and conceptual boundaries has resulted in research, education and practice*

[18] KALMAN, T. (1991), Good History, Bad History, *Design Review*, 1(1), pp. 44-57, as cited in BARNARD, M. (2013), Graphic Design as communication. In Routledge eBooks. https://doi.org/10.4324/9781315015385, p. 10

[19] RODGERS, P. A., & BREMNER, C. (2017). The concept of the design discipline. Dialectic, I(1). https://doi.org/10.3998/dialectic.14932326.0001.104, pp. 21-22.

[20] LATOUR, B. (2012). 9. A Cautious Prometheus? A Few Steps Toward a Philosophy of Design with Special Attention to Peter Sloterdijk. In Amsterdam University Press eBooks (pp. 151–164). https://doi.org/10.1515/9789048514502-009, p. 3. On the same note, this author also states that the expansion of design has been so enormous that designing something may very well equate to *planning, calculating, arraying, defining, or projecting something.*

[21] LATOUR, B. (2012), *ibid*, pp.1-2

[22] What is design? (n.d.). International Council of Design. https://www.theicod.org/en/professional-design/what-is-design/what-is-design

[23] This is backed by the fact that persuasion is, quite literally, one of the main functions of graphic design. See BARNARD, M. (2013), *ibid*, p. *15.*

[24] Brignull, H. (2023) Deceptive patterns: Exposing the Tricks Tech Companies Use to Control You. Testimonium Limited, p. 13

[25] RODGERS, P. A., & BREMNER, C. (2017), *ibid*, p. 22.

that is constantly shifting, creating, contesting and negotiating new terrains of opportunity and re-shaping the boundaries of design[26] [27]*".*

Given the scope of this dissertation, we will be focusing on digital design, solely. This particular branch of graphic design refers to the planned way information is presented – or communicated - to a user on an electronical device. There are several types of digital design, such as web and app design, UI and UX design, infographic design, email design, social media design, 3D design, etc. As previously stated, we will not cover all of these types here, for the aforementioned reason, and will only be talking about the first three examples: Web and app design encompass various elements, including interaction design, which further breaks down into UI design and UX design.

Web design refers to the design of websites (and apps, when in regards to app design) and, typically, refers to the user experience aspects of website development and not so much to the software development. Interaction design, in turn and very simply put, "*is about shaping digital things for people's use*[28]*".* Both these fields emerged with the advent of the internet and of the first websites[29], circa the turn of the century, but as digital interactive consumer products grew, so did interaction design and the concern for crafting these products with a greater focus on the user experience rather than solely on the usability and efficiency of websites and/or other digital platforms[30].

Therefore, we will adopt the ICD's definition of 'design'[31], for considering what has been exposed and its inherent function of communication, we consider it to be one of the most complete notions.

[26] RODGERS, P. A., & BREMNER, C. (2017), *ibid*, pp. 22-23.
[27] RODGERS, P., & BREMNER, C. (2011). Alterplinarity: "Alternative Disciplinarity" in Future Art and Design Research Pursuits. Studies in Material Thinking, 6, 1–16. http://nrl.northumbria.ac.uk/7436/2/Alterplinarity_PaulRodgers.pdf
[28] LOWGREN, J. (2014). Interaction Design - brief intro. Interaction Design Foundation - IxDF. https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/interaction-design-brief-intro
[29] MEGGS, P. B. (2024). graphic design. Encyclopedia Britannica. https://www.britannica.com/art/graphic-design. As this author highlights, "*the digital revolution in graphic design was followed quickly by public access to the internet".* Unlike designing for print, designing for the web involves considering the usage of hyperlinks and the navigation of the platform.
[30] LOWGREN, J. (2014), *ibid.*
[31] As mentioned above, for the ICD, design is *a discipline of study and practice focused on the interaction between a person — a 'user'— and the man-made environment, taking into account aesthetic, functional, contextual, cultural and societal considerations.*

Principles of design

Such as law has its own set of guiding principles and rules, so does design. Seeing as deceptive design patterns are built by exploiting these principles, as mentioned on the introduction, it is useful to enumerate and explain them before proceeding to the next section of our dissertation. The main principles of design are balance, proportion, alignment, contrast, emphasis, repetition, hierarchy, and unity[32] [33]. Two notes are required before proceeding: one, principles are exactly that – guidelines. That means that they are not set in stone and can change or be worded differently from source to source. In this dissertation, we simple chose the ones that appear to be the most widely regarded as the main design principles.

The second note is regarding the *Gestalt* Principles (or Gestalt laws of perceptual organization). The *Gestalt* principles are "laws of human perception that describe how humans group similar objects, recognize patterns and simplify complex images when perceiving objects[34]" for we need to understand them in order to understand how they are used by designers. Gestalt means *united whole*, in german, and these principles were built circa 1920 by a group of german pyschologists called Max Wertheimer, Kurt Koffka and Wolfgang Kohler[35], having been applied in user interface design, graphic design, and information visualization ever since[36]. These principles originated from the discovery of phenomenal (phi) motion, by Wertheimer, in 1912, a theory built from apparent motion, in which he demonstrated that the human eye observes motion when two or more nearby optical stimuli are presented alternatively at a relatively high frequency[37], even when, in

[32] BANDLI, S. (2021) How the 8 design principles should be applied to learning. https://elearningindustry.com/how-apply-design-principles-to-online-learning.
[33] CorelDRAW Graphics Suite | Free Trial (no date b). https://www.coreldraw.com/en/tips/graphic-design-principles/#principles.
[34] Interaction Design Foundation - IxDF. (2016, August 30). What are the Gestalt Principles?. Interaction Design Foundation - IxDF. https://www.interaction-design.org/literature/topics/gestalt-principles
[35] Ibid.
[36] KOBOUROV, S.G., MCHEDLIDZE, T., VONESSEN, L. (2015). Gestalt Principles in Graph Drawing. In: Di Giacomo, E., LUBIW, A. (eds) Graph Drawing and Network Visualization. GD 2015. Lecture Notes in Computer Science(), vol 9411. Springer, Cham. https://doi.org/10.1007/978-3-319-27261-0_50, p.1
[37] WAGEMANS, J., ELDER, J. H., KUBOVY, M., PALMER, S. E., PETERSON, M. A., SINGH, M., & VON DER HEYDT, R. (2012). A century of Gestalt psychology in visual perception: I. Perceptual grouping and figure–ground organization. Psychological Bulletin, 138(6), 1172–1217. https://doi.org/10.1037/a0029333, p.1. The experiment was conducted as following: *"(…) a white strip was placed on a dark background in each of two slits in the wheel of a tachistoscope, and the rotation speed was adjusted to vary the time required for the light to pass from one slit to the next (i.e., the interval between the two). Above a certain threshold value (~200 ms), observers saw the two lines in succession. With much shorter intervals (~30 ms), the two lines appeared to flash simultaneously. At the optimal stage (~60 ms), observers perceived a motion that could not be distinguished from real motion. When the interval was decreased slightly below 60 ms, after*

reality, no motion is present. From this point, he came to the conclusion that "structured wholes or *Gestalten*, rather than sensations, are the primary units of mental life[38]", emphasizing the idea that "the whole of anything is greater than its parts[39]" and the two might not even be related to each other.

The more common principles, according to cited works of the Interaction Design Foundation, are twelve: emergence, closure, common region, continuity, proximity, multistability, figure/ground, invariance, *prägnanz* (or good figure), similarity, symmetry, and common fate[40].

The principle of emergence is correlated to the way the human brain is wired to make sense out of what surrounds us in a general way, configuring "whole, meaningful objects[41]" (perceiving the whole) without being too overly concerned about fine details (unconsciously ignoring the parts)[42].

Closure, sometimes also referred to as reification, pertains the way the human brain "perceive elements as belonging to the same group if they seem to complete some entity[43]". Once again, this principle shows us that humans subconsciously see the entirety of a shape before seeing anything else[44].

The principle of common region states that if a lot of items are placed within the same boundary, then those items will be perceived as part of a single unity and, thus, "assumed to share some common characteristic[45]". The law of common fate is quite similar, but it is applied, usually, to moving graphics as it takes advantage of how "human nature associates objects that share a common motion[46]" as a unified group.

---

repeated exposures, observers perceived motion without a moving object—that is, pure phenomenal or phi motion."

[38] Ibid.

[39] MSEd, K. C. (2024, April 22). What are the gestalt principles? Verywell Mind. https://www.verywellmind.com/gestalt-laws-of-perceptual-organization-2795835

[40] Interaction Design Foundation – IxDF (2016, Augusto 30), ob. cit.

[41] LUDICK, I. (2019, July 5). Design principles: Gestalt Psychology. https://www.linkedin.com/pulse/design-principles-gestalt-psychology-ian-ludick

[42] Typical examples used by scholars to illustrate this principle are the figure of the dalmatian on the woods, which, albeit being composed by random blobs and shapes, shows how our eye automatically perceives the dog. Another example is the unilever logo, which is the letter "U" made out of several other smaller icons.

[43] KIM, B., REIF, E., WATTENBERG, M., BENGIO, S., & MOZER, M. C. (2021). Neural networks trained on natural scenes exhibit gestalt closure. Computational Brain & Behavior, 4(3), 251–263. https://doi.org/10.1007/s42113-021-00100-7, as cited in MSEd, K. C. (2024, April 22).

[44] Interaction Design Foundation - IxDF. (2016, August 30). What are the Gestalt Principles?. Interaction Design Foundation - IxDF. https://www.interaction-design.org/literature/topics/gestalt-principles, ob. cit.

[45] HARLEY, A. (2023, March 6). The principle of common region: containers create groupings. Nielsen Norman Group. https://www.nngroup.com/articles/common-region/, available at https://www.nngroup.com/articles/common-region/

[46] What is the Law of Common Fate? (2024, June 20). The Interaction Design Foundation. https://www.interaction-design.org/literature/topics/law-of-common-fate

Continuity, or continuation, originates from our eye's tendency to "follow the smoothest path when observing lines[47]", and fill the missing information to form a whole figure or perceive a "continuous flow of visual elements[48]" rather than segregated ones.

The principle of proximity states that items closed to each other are perceived as related[49]. This principle can be connected to the principle of similarity, which states that objects sharing similar characteristics will, too, be perceived as a group[50]. The same idea lingers behind the principle of similarity – the human brain prefers symmetrical forms over asymmetrical ones, and thus, we perceive objects as part of the same whole if they are arranged in a symmetrical fashion[51].

Continuing this brief enumeration of gestalt's laws of human perception, we can move along to the law of multistability, or multistable perception, which happens when we are presented with an image that is ambiguous, such as the Rubin's vase, for example. As our brain cannot process two versions of something at the same time, we experience "the sensation of switching between them"[52]. This principle is sometimes confused with Figure/Ground, but while the former happens with ambiguous images or objects, the latter is related to the way the human eye tends to see the foreground (the figure) before perceiving the background (the ground), as, typically, that is where the most important objects are located[53]. To distinguish the figure from the background, designers usually resort to applying techniques such as blurriness, contrast, size, and separation[54].

Invariance, the next principle we will describe, regards the brain's ability to recognize certain objects, in spite of rotation or distortion, for example[55].

Lastly, we have decided to leave the principle of *prägnanz* (or good figure) to the end, as it is the one which wraps up all the other mentioned principles. The word in itself can be translated to precision or to cohesion, and describes the way we process

---

[47] What is the Law of Continuity? (2024, June 28). The Interaction Design Foundation. https://www.interaction-design.org/literature/topics/law-of-continuity

[48] Ibid.

[49] Lumen Learning. (n.d.). Gestalt Principles of Perception | Introduction to Psychology. https://courses.lumenlearning.com/waymaker-psychology/chapter/gestalt-principles-of-perception/

[50] Interaction Design Foundation - IxDF. (2016, August 30). What are the Gestalt Principles?. Interaction Design Foundation - IxDF. https://www.interaction-design.org/literature/topics/gestalt-principles, ob. cit.

[51] Ibid.

[52] Ibid.

[53] MSEd, K. C. (2023, September 7). Figure-Ground perception in Psychology. Verywell Mind. https://www.verywellmind.com/what-is-figure-ground-perception-2795195

[54] Ibid.

[55] GASKIN, J. (2024, June 13). What are gestalt design principles? A complete breakdown. Venngage. https://venngage.com/blog/gestalt-principles/#in

information: in a quick, succinct way[56], with a tendency to simplify otherwise complex forms and shapes because we are averse to chaos, as mentioned above[57].

Coming to the end of the very brief and humble introduction we made to the Gestalt principles and psychology, we are now able to proceed to explaining the aforementioned principles of design, and how they all relate to the idea that the way humans perceive the world around them is not always the most precise one – just the easiest, most times. Therefore, it makes sense that designers should design with this idea in mind, especially when doing so for user experience and interaction.

Now that we have enumerated the *Gestalt* laws of human perception, we can look at some basic principles of graphic design that are usually followed by designers in their compositions.

We will start with the principle of emphasis, as it can be seen as the base for all the others, for "it means having a focal point[58]" for the design. Lines, colors, alignment, contrast, and repetition can all be tools used to build that focal point to lead the user's attention there and, eventually, to make them do something[59]. The principle of hierarchy, too, plays a pivotal line in showing users precisely what the designer wants them to pay attention to[60]. Simply put, and much like emphasis, in order to establish hierarchy, a designer must take advantage of all the other elemental principles[61] in order to show the order of importance of the elements on a specific design, as this is how, "by laying out elements logically and strategically, designers influence users' perceptions and guide them to desired actions[62]". An effective use of hierarchy aims to "inform, impress and persuade users[63]" and their expectations when using a certain website or landing page.

The principle of balance, in very concise terms, is about arranging the elements on a design "to create satisfaction, completion and cohesion[64]". Balance, along with unity,

---

[56] GASKIN, J. (2024, June 13). What is the law of Pragnanz? A complete breakdown. Venngage. https://venngage.com/blog/law-of-pragnanz/

[57] What is the Law of Prägnanz? (2024, June 28). The Interaction Design Foundation. https://www.interaction-design.org/literature/topics/law-of-praegnanz

[58] CorelDRAW Graphics Suite | Free Trial (no date e). https://www.coreldraw.com/en/tips/graphic-design-principles/emphasis/.

[59] Ibid.

[60] CorelDRAW Graphics Suite | Free Trial (no date). https://www.coreldraw.com/en/tips/graphic-design-principles/hierarchy/.

[61] By manipulating principles such as size, color, contrast, alignment, repetition, proximity, and negative space, for example.

[62] What is Visual Hierarchy? (2024, February 11). The Interaction Design Foundation. https://www.interaction-design.org/literature/topics/visual-hierarchy

[63] Ibid.

[64] CorelDRAW Graphics Suite | Free Trial (no date). https://www.coreldraw.com/en/tips/graphic-design-principles/balance/.

is what creates in the user the idea that certain elements are related which is why this principle is useful in guiding the way (and where) the user looks at, for example, a website page.

Proportion relates "to the relative size of the elements in graphic design[65]" and, unlike balance, which pertains more to the arrangement and visual weight of the elements on a page, the principle of proportion is about the relational size and scale of the elements with each other. This might be one of the easiest principles to explain when it comes to the topic of our dissertation – typically, our attention is drawn to bigger shapes and text, so it is quite easy to hide important information in small (often with lower contrast) text, whereas we display anything else in big bold letters to lead the user's attention there instead of to the actually important information. We will return to this later, when discussing the categorization of deceptive design patterns.

Moving along to the next principle, alignment is a subtle, but important principle: even though it relates to the "lining of graphics and text in relation to the various edges of the canvas[66]", it has a crucial importance in, once more, guiding the way a user reads the information on a page. Left alignment is what most people expect, center alignment is a way to make information stand out and items aligned to the right usually are complementary – when an important piece of information is unexpectedly aligned to the right, it can be simple for the user to overlook it in detriment of other elements present on the page.

In graphic design, contrast "is the visible difference in properties of the design elements[67]" and it serves the purpose to determine the first thing that will be visible to the viewer[68], thus creating a more effective form of communication.

The principle of repetition brings familiarity to a design – it lets the user know what to expect. In the specific case of digital design, when entering a website, most users know where to expect the brand's logo to be, or where the menus, or search bar, might

[65] Ibid.
[66] CorelDRAW Graphics Suite | Free Trial (no date c). https://www.coreldraw.com/en/tips/graphic-design-principles/alignment/.
[67] CorelDRAW Graphics Suite | Free Trial (no date d). https://www.coreldraw.com/en/tips/graphic-design-principles/contrast/.
[68] Ibid.

be[69] and those expectations end up reflecting themselves on the way designers build websites[70].

In this subsection we analyzed the psychology of gestalt, which describes that the human brain seeks to simplify what it sees and usually perceives the whole, rather than what constitutes it, as that is the simplest, quickest and more economical way to traverse life. We briefly described the twelve laws, or principles, on which this school was built on, and how they should be applied to design; especially in UI and UX. Afterwards, we chose to summarize the eight principles of design, as they seem to be a practical application of the laws of gestalt and constitute 'good design' as it respects how the human brain expects to see information and understands it. Therefore, the misapplication of these principles in building a certain interface will result in bad design. If done so with the intention of deceiving the user, then we will surely be in the presence of deceptive design.

Cognitive biases, however, are also extremely important for the proper comprehension of deceptive design patterns and thus, that is what the following subsection of this chapter will focus on.

The psychology behind deceptive design – limits of the human brain

Cognitive bounds

The need to explain the way real-life behavior differs from the outcome reached by traditional economic models based on assumptions was the foundation for the development of the science of behavioral economics[71]. Behavioral economics uses psychology, neuroscience and sociology to explain human behavior and thus, it proves that it is not possible to explain it based on pre-established theories and without looking at each motive and intention[72].

[69] CorelDRAW Graphics Suite | Free Trial (no date f). https://www.coreldraw.com/en/tips/graphic-design-principles/repetition/.
[70] NIKOLAUS, U. & BOHNERT, S.: (2017) User Expectations vs. Web Design Patterns: User Expectations for the Location of Web Objects Revisited. Conference Proceedings after HFES Europe Annual Conference. https://www.hfes-europe.org/wp-content/uploads/2017/10/Nikolaus2017poster.pdf
[71] THALER, R. H. (2015). Misbehaving: the making of behavioral economics. *Choice Reviews Online*, *53*(01), 53–0352. https://doi.org/10.5860/choice.192072, as cited by REYNA, A. (2018). The psychology of privacy—what can Behavioural Economics contribute to competition in digital markets? *International Data Privacy Law*, *8*(3), 240–252. https://doi.org/10.1093/idpl/ipy017, p. 242
[72] REYNA, A. (2018), ob. Cit., p. 242

The rational choice theory assumes that human decision-making processes can be explained from the viewpoint of maximization of the utility gained from one choice instead of another. Thus, according to these theories, "all actors are rational, have willpower and act on their self-interest[73]."

Real people, however, are not that straightforward in their decision-making processes, and are far more complex than the *homo economicus.* Regarding their privacy, in particular, there is a significant discrepancy between how consumers are expected to behave and how they actually do[74]. According to THALER, SUSTEIN and JOLLS, people deviate from the outcomes predicted by the traditional rational choice theory through three cognitive bounds: bounded rationality, bounded willpower, and bounded self-interest[75].

Bounded rationality says that, when making a decision, people are influenced by their own beliefs and perceptions of themselves and their surroundings, therefore not relying exclusively on the available information, because "human cognitive abilities are not infinite[76]".

Bounded willpower happens when people make a decision that might go against their best interest and have an unpredictable outcome, but the benefits they might reap outweighs the costs. This bound is a mechanism people adopt to mitigate the effects of their limited willpower[77].

Lastly, bounded self-interest is connected with the idea that people act benevolently, even if that is not in their best financial interest out of caring (or pretending to care) for each other[78].

---

[73] BECKER, G. S. (1976). *The economic approach to human behavior*. https://doi.org/10.7208/chicago/9780226217062.001.0001, pp. 3-14, as cited by REYNA, A. (2018) ob. cit, p. 242.

[74] REYNA, A. (2018), ob. Cit., p. 241. As an example, the author uses the Facebook-Cambridge Analytica scandal and how most users continued to use facebook as usual.

[75] JOLLS, C., SUNSTEIN, C. R., & THALER, R. H. (July 1998), *A behavioral approach to law and economics*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=74927, p. 1476, available on A Behavioral Approach to Law and Economics (uchicago.edu)

[76] SIMON, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, *69*(1), 99. https://doi.org/10.2307/1884852, as cited by JOLLS, C., SUNSTEIN, C. R., & THALER, R. H. (July 1998, ob. cit., p. 1477

[77] JOLLS, C., SUNSTEIN, C. R., & THALER, R. H. (July 1998), ob. cit., p. 1479

[78] Ibid.

Cognitive biases

KAHNEMAN has argued (and demonstrated) that humans have two distinct systems of thinking: one that "operates automatically and quickly, with little to no effort and no sense of voluntary control[79]", and another, which, in turn, "allocates attention to the effortful mental activities that demand it (…)[80]" being thus associated with activities that require our full "agency, choice and concentration[81]". The same author then explains that most times we think and act with the first one, which not only entails our innate skills (perception of the world around us, object recognition, etc.) but also what allows us to create association between ideas and intuitively perceiving social cues without exhausting ourselves, because of our limited attention capacity[82]. The interaction between the two systems usually works quite well, because "it minimizes efforts and optimizes performance", but the first system – also called heuristics- is subject to some errors, at times, due to force of habit. These errors are cognitive biases.

Cognitive biases are psychological phenomena that can be described as "systematic, universally occurring, tendencies, inclinations, or dispositions in human decision making that may make it vulnerable for inaccurate, suboptimal, or wrong outcomes[83]" which result from our heuristics' (the mental shortcuts we take in order to simplify and minimize the mental load of "assessing probabilities and predicting values[84]" given our limited time and attention) failure to form a correct judgment. Cognitive biases are naturally occurring and typical, given our limited cognitive capacity, and asymmetrical, as we usually do not perceive our own incurrence in these biases, and thus fail to realize how we are being influenced by them[85]. As cognitive biases work as "intuitive, tacit knowledge[86]" and thus, if used against the user, can do more harm than good, as we will demonstrate.

---

[79] KAHNEMAN, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux. p. 22.
[80] Ibid.
[81] Ibid.
[82] Ibid, pp. 24-25
[83] KORTELING, J. E., PARADIES, G. L., & MEER, J. P. S. (2023). Cognitive bias and how to improve sustainable decision making. *Frontiers in Psychology*, *14*. https://doi.org/10.3389/fpsyg.2023.1129835 , p. 2.
[84] TVERSKY, A., & KAHNEMAN, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124, p. 1124.
[85] PRONIN, E., LIN, D. Y., & ROSS, L. (2002). The Bias Blind Spot: perceptions of bias in self versus others. *Personality and Social Psychology Bulletin*, *28*(3), 369–381. https://doi.org/10.1177/0146167202286008, p. 370.
[86] HILDEBRANDT, M. (2019). The issue of bias. The framing powers of ML. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3497597, pp. 9-10

Assuming that, throughout the years, more than one hundred cognitive biases have been identified by scholars[87], we will only focus on those that are relevant to the development of deceptive design patterns.

The first we will mention is anchoring-and-adjustment, which defines the psychological process of relying disproportionately on information readily available to make a decision[88]. The reason why this bias is so predictable in estimates is because "one's initial anchor tends to be insufficient[89]", thus rendering the initial judgement inexact. A quick example of this bias in deceptive patterns can be the usage of false information on websites to persuade users to disclose more information than what they would initially do by, *v.g.*, stating that, for example, *3 out of 5 users choose to share their mobile phone number when registering to this website.*

Framing is another example of a widely used cognitive bias and concerns the way information is presented to the user, usually associated with a valuation judgement[90]. As we are typically risk-averse creatures, a potential loss tends to outweigh a potential win. The example used by WALDMAN is particularly illustrative of this tactic: by making a statement as simple as "if you don't allow cookies, website functionality will be diminished" or "opting in to data collection will enable new and easier functionality" is usually enough to make sure that users consent to their data being processed because there is a certain reward perceived[91].

In third place, we can mention hyperbolic discounting as another bias that can be taken advantage of when designing websites with deceptive design patterns. Typically, our brain tends to value more the short-term effects of a decision than the long-term ones[92] - as illustrated by the cited author, in a study conducted by JENTZCH et al, it was discovered that people preferred to pay a lower price for movie tickets, even if that meant sharing more personal data. On the contrary, if the price was the same, then people would prefer the most privacy friendly company selling the tickets[93].

---

[87] EHRLINGER, J., READINGER, W., & KIM, B. (2016). Decision-Making and cognitive biases. In Elsevier eBooks (pp. 5–12). https://doi.org/10.1016/b978-0-12-397045-9.00206-8, p. 4
[88] WALDMAN, A. E., (September 18, 2019). Cognitive Biases, Dark Patterns, and the 'Privacy Paradox' 31 Current Issues in Psychology 2020, Available at SSRN: https://ssrn.com/abstract=3456155, p. 3.
[89] EHRLINGER, J., READINGER, W., & KIM, B. (2016), op. Cit. p. 6
[90] WALDMAN, A. E., (September 18, 2019), op. cit., p. 6
[91] Ibid.
[92] Ibid.
[93] JENTZSCH N., PREIBUSCH S., HARASSER A.: Study on Monetising Privacy: An Economic Model for Pricing Personal Information. European Union Agency for Network and Inf. Sec. (ENISA), as cited in Ibid, p. 7.

Choice overload (or *overchoice*) is yet another cognitive bias, as noted by WALDMAN, due to the amount of choices we have to make and navigate through (cookie consent, tracking and personalized advertising, for example) on a daily basis. As it has been studied by this author, not only does the number of choices available exhaust our mental energy, but it also makes us want to "decline to manage" our own data online[94], conforming to the default option.

In fourth place, we can point out the social proof bias as a major driver for the use of deceptive patterns that rely on human's tendency to conform, particularly in situations of uncertainty, because people assume the actions of others as the correct way to behave or act[95]. Due to what has been exposed, this bias can be especially powerful when used together with choice overload, because if there are too many options to choose from (which leads us to mental exhaustion and defaulting to the preselected one, which is exacerbated due to our default bias[96]), it becomes easier to nudge us towards a certain choice if we add, for example, reviews of it or a statement that says something as simple as *100 people bought this product recently (which means you should, too).*

MATHUR et al. also highlight the sunk-cost fallacy as another cognitive bias that is present in the use of deceptive patterns, and it describes "the tendency of individuals to continue an action if they have invested resources into it, even if that action might make them worse off[97]". Additionally, the scarcity bias, which states that we value something more if we believe it to be scarce, can also play a huge role in manipulating users[98].

We can conclude this section by stating that there are many ways that a company can take advantage of these biases and of the way humans perceive the world around them. Our behavior is not linear nor entirely logical, we are hard-wired to think intuitively

[94] WALDMAN, A. E., (September 18, 2019), op. cit., p. 7

[95] Wintermeier, N. (2023, February 7). Social Proof Examples: The Powerful Psychological Bias in Marketing. Crobox. https://blog.crobox.com/article/social-proof-examples

[96] By the Power of Default. Center for Advanced Hindsight (2018, June 13). https://advanced-hindsight.com/blog/by-the-power-of-default/. Our tendency to stick to the *status quo*, as that is what involves less mental effort and what is the most similar to our previously made decisions. To see more on this bias,

[97] MATHUR, A. et al. (2019) "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites," Lirias (KU Leuven), 3, Article 81, p. 6. Available at: https://lirias.kuleuven.be/handle/123456789/659030.

[98] CIALDINI, R.B. (2008). Influence: Science and Practice, 5th ed. Boston: Pearson, as cited in BehavioralEconomics.com. (2023, February 24). Scarcity (heuristic) - BehavioralEconomics.com | The BE Hub. BehavioralEconomics.com | the BE Hub. https://www.behavioraleconomics.com/resources/mini-encyclopedia-of-be/scarcity-heuristic/

and automatically, and that is precisely what makes us predictable – and vulnerable - to be manipulated[99] by companies who wish to profit above all else.

Deceptive design patterns – evolution & categorization

The usage of deceptive design patterns has become more common due to not only the massification of the access to internet, but also to the consequent rise of the metrics-driven culture, the fact that it is easier than ever to track people and their online behavior and also to run A/B tests without too much effort[100]. As it gradually became easier than ever to know what people are doing and/or looking at on their screens, it soon became clear that it was far simpler – and more profitable – to find ways to persuade users to give away their personal data for targeted advertisement by taking advantage of the way the human brain works than by effectively seeking valid consent (by, for example, making the "accept all" cookies consent button more prominent than the "do not accept any" or the "personalize options" ones[101]), the path was set.

The term "dark patterns" was originally coined by BRIGNULL in 2010, with the creation of deceptive.design.org, as a way to name-and-shame the companies (mostly e-commerce ones) that employed these tactics to manipulate consumers by subverting the principles we analyzed above and taking advantage of the way our brain processes information, also briefly explained in the previous sections.

That said, there are several kinds of deceptive patterns and, also, several ways to categorize them. The EDPB Guidelines 03/2022, for example, categorize them into five distinct categories: overloading, skipping, hindering, fickle and left in the dark[102].

---

[99] HARRIS, T. (2019, October 16). How Technology is Hijacking Your Mind — from a Magician and Google Design Ethicist. Medium. https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3

[100] Brignull, H. (2023), op.cit., pp. 19-22

[101] GRASSL, P., SCHRAFFENBERGER, H., BORGESIUS, F. Z., & BUIJZEN, M. (2020). Dark and bright patterns in cookie consent requests. Journal of Digital Social Research, 3(1), 1–38, p. 24, https://doi.org/10.31234/osf.io/gqs5h. These authors conducted a study in which they concluded, unsurprisingly, that the usage of deceptive patterns on cookie consent dialogs substantially influenced the users' response.

[102] Guidelines 03/2022, p. 10. Among many others, they identify, under Overloading, the Continuous Prompting, Privacy Maze and Too Many Options. Under skipping, the Emotional Steering and Hidden in Plain Sight tactics are listed as commonly used patterns. Under hindering, we can find Dead End, Longer than Necessary and Misleading Information. Under fickle, we can find Lacking Hierarchy and Decontextualizing and, finally, under left in the dark we can find Language Discontinuity, Conflicting Information and Ambiguous Wording/Information.

The French National Data Protection Authority (hereinafter, CNIL), in the aforementioned report, propose four categories of deceptive patterns (pushing the individual to accept sharing more than what is strictly necessary, influence consent, creating friction on data protection actions and diverting the individual) and five ways to implement these (enjoy, seduce, lure, complicate and ban)[103].

BOSCH et al., on their hand, propose a system based on the privacy strategies identified by HOEPMAN[104]. The categorization proposed by these authors denotes an antagonizing relationship between privacy strategies and privacy dark strategies, thus identifying the following strategies as dark: maximize, publish, centralize, preserve, obscure, deny, violate, and fake[105]. It is worth mentioning that several scholars have also been working on analyzing mobile apps, such as "pay to skip[106]".

BRIGNULL, on his project, proposes sixteen categories of deceptive design patterns: comparison prevention, *confirmshaming*, disguised ads, fake scarcity, fake social proof, fake urgency, forced action, hard to cancel, hidden costs, hidden subscription, nagging, obstruction, preselection, sneaking, trick wording and visual interference[107]. The taxonomy followed by this author is the one created by MATHUR et al.[108], and thus, given his expertise and knowledge on the matter, along with that which is proposed by the EDPB, are the ones we will be following for the purpose of this dissertation.

[103] CHATELLIER, R., DELCROIX, G. HARY, E., et al., (2019) *op. cit.*, p. 28. Under the first category, we can find Safety Blackmail, Just between You and Us, False Continuity, Improving the Experience and Default Sharing. Under influence consent, we find Trick Question, Last Minute Consent, Attention Diversion, Comparison Obfuscation and Wrong Signal. Under the creating friction on Data Protection Actions, we can find Blaming the Individual, Impenetrable Wall, Making it Fastidious to Adjust Confidential Settings, Repetitive Incentive and Obfuscating Settings. Finally, under Diverting the Individual, we find Bait and Change, Chameleon Strategy and Camouflaged Advertising.

[104] HOEPMAN, J.-H. (2014) "Privacy Design Strategies," in IFIP advances in information and communication technology. Springer Science+Business Media, pp. 446–459, pp. 455-458. Available at: https://doi.org/10.1007/978-3-642-55415-5_38. Hoepman identifies the following strategies to be implemented in UI: minimize, hide, separate, aggregate, inform, control, enforce and demonstrate.

[105] BÖSCH, C. et al. (2016) "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns," Proceedings on Privacy Enhancing Technologies, 2016(4), pp. 237–254, pp. 241, 243-244. Available at: https://doi.org/10.1515/popets-2016-0038.

[106] LEWIS, C. (2014). Irresistible apps. In Apress eBooks. https://doi.org/10.1007/978-1-4302-6422-4, as cited in MATHUR et. al, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites," Lirias (KU Leuven), 3, Article 81, Available at: https://lirias.kuleuven.be/handle/123456789/659030, p. 4.

[107] BRIGNULL, H., Deceptive Patterns - Types of Deceptive Patterns (2023). Available at: https://www.deceptive.design/types.

[108] Mathur, A. et al. (2019) ob. cit., p. 3

MATHUR et al. categorize deceptive patterns in five ways: asymmetric, covert, obstructive, deceptive, and restrictive, depending on the effect they have on the user and on the way they are designed[109].

Asymmetric patterns seem to be designed with a subversion of the principles of balance, proportion and contrast in mind, for typically the platform's architecture is built in a way in which the user will be more inclined to choose one option instead of the other (for example, by presenting a large, red button to accept cookies, but making the opt-out button less visible or with too many options[110]), which also facilitates the incurrence in the default effect cognitive bias.

Covert patterns hide from the user the true effect of the user interface design choice, which means that platforms built with these kinds of patterns may nudge users towards making certain choices without their knowledge[111], thus extrapolating the anchoring-and-adjustment and framing biases.

Patterns that employ deception tactics "induce false beliefs either through affirmative misstatements, misleading statements or omissions[112]", for example, making users believe – most times, falsely – that they have a limited time to enjoy a special discount, or that other people are making the same choices as them. These patterns typically make users incur in the social proof bias, as well as on the sunk-cost fallacy.

Obstructive patterns hide the information from users, plain and simple, or make it difficult for the user to get it[113]. These patterns may exploit the sunk-cost fallacy, the default effect or the choice overload biases, for example.

Lastly, restrictive patterns are pretty self-explanatory – the platform is built in such a way that users, for example, are prevented from making certain choices on purpose[114].

Now that we have briefly explained the categorization we will use, we are apt to move along to the deceptive patterns themselves.

Comparison prevention is a type of obstructive deceptive pattern in which the user finds difficulty in comparing products on an interface due to the overly complicated manner in which the features and prices are combined, or in finding essential

[109] Ibid., p. 6.
[110] Ibid., p. 5.
[111] Ibid.
[112] Ibid.
[113] Ibid., p. 6
[114] Ibid.

information[115]. As we explained above, making a choice when there are too many options to weight exhaust us, and thus makes us more vulnerable to cognitive biases such as social proof or the default effect.

Confirmshaming is an asymmetric deceptive pattern which "works by triggering uncomfortable emotions, such as guilt or shame, to influence users' decision-making[116]". In our opinion, and in line with the EDPB's outlook on this practice, confirmshaming does not rely exclusively on negative emotions, but also on positive ones, referring to these practices as emotional steering[117], which can make users incur in the framing bias.

The **disguised ads** pattern employs deception by making users believe they are clicking on actual content, while instead, they are clicking on advertisements in order to, on the one hand, generate more revenue for the platform, and on the other, generate higher clickthrough rates for the advertiser[118].

Following, we have the **fake scarcity, fake social proof,** and **fake urgency** patterns. Due to their deceptive nature, we can start by stating that all of these take full advantage of the scarcity bias, as well as of social proof and of the anchoring-and-adjustment bias, as well as the hyperbolic-discount one. Firstly, what all of these patterns have in common their fake nature. In fake scarcity, users are led to believe that a product or a service has limited availability, as either high demand or low-stock messages are displayed near the items[119]. With fake social proof, platforms prey on our tendency to conform to others' behavior – and deeming it correct - by creating a false sense of popularity of a service or product by resorting to fake and/or exaggerated testimonials and reviews[120]. Lastly, with fake urgency, as "the user is placed under time pressure, they are less able to critically evaluate the information shown to them because they have less time and may experience anxiety or stress[121]", which can be easily achieved by using fake countdown timers or fake text embed in the platform itself[122]. As MATHUR et al. confirm, these patterns can also be classified as partially covert, beyond being deceptive[123].

[115] Deceptive patterns - Types of deceptive pattern. (n.d.-b). https://www.deceptive.design/types
[116] Deceptive Patterns - types - Confirmshaming. (n.d.). https://www.deceptive.design/types/confirmshaming
[117] EDPB Guidelines 03/2022, pp. 19-20
[118] Deceptive Patterns - types – Disguised ads. (n.d.).
[119] Deceptive Patterns - types – Fake scarcity (n.d.).
[120] Deceptive Patterns - types – Fake social proof (n.d.).
[121] Deceptive Patterns - types – Fake urgency (n.d.).
[122] MATHUR et. al, op. cit., pp. 15-16
[123] Ibid., p. 16

Continuing our analysis, comes the **forced action** deceptive pattern, which "involves a provider offering users something they want, but requiring them to do something undesirable in return[124]" such as giving their consent for multiple ends in one single action (what BRIGNULL refers to as "bundled consent[125]"). As the same author notes, this pattern is problematic as it contradicts the user's expectations[126], and, ultimately, can result in the user not being fully aware of what they are consenting to, or what kind of data will be processed, with whom, and for what ends, which ultimately violates the GDPR and its principles, as we will argue on the following part of this dissertation. It is an asymmetrical deceptive pattern, for the user is mostly – if not completely - left in the dark in regards to the company's intentions in regards to their data (thus creating a power imbalance) and also a restrictive one, for the user might find difficulty in choosing a stance that is more privacy-friendly because they are forced to subscribe for services they do not want, such as marketing communications, as highlighted by MATHUR et al[127]. These patterns prey on our default bias and choice overload biases.

Following, we can mention the **obstruction** deceptive pattern, in which the company "deliberately creates obstacles or roadblocks in the user's path, making it more difficult for them to complete the desired action[128]" or simply to tire them, thus making them more susceptible to being further manipulated due to exhaustion or frustration[129]. It is an obstructive pattern, for it specifically prevents user autonomy.

Next, we will talk about the **hard to cancel** pattern, which we include in the obstructive patterns category, and regard practices in which companies incur in order to purposefully make the unsubscription process or the cancellation of a service more difficult than it needs to be[130]. This can be achieved by either forcing the consumer to have to communicate with customer support or back-office support in order to cancel the service provision, or by adding extra steps to the unsubscription process. As we mentioned above, most people have limited time and attention and thus, by overcomplicating a process, some might end up giving up or delaying the decision to

[124] Deceptive Patterns - types – Forced Action(n.d.).
[125] Ibid.
[126] BRIGNULL, H. (2023), op. cit., p. 152
[127] MATHUR et. al, op. cit., p. 22
[128] Deceptive Patterns - types – Obstruction (n.d.).
[129] Ibid.
[130] Deceptive Patterns - types – Hard to cancel (n.d.).

unsubscribe, thus rendering more company more revenue – even if for just one more month. Although MATHUR et al. include this pattern inside the obstruction one, without separating them[131], we agree with BRIGNULL and consider it a different deceptive pattern, in spite of the similarities, as the hard to cancel pattern is specific to certain situations (namely, the cancellation of services), whereas the obstruction pattern has a broader meaning, in our opinion.

The **hidden costs** pattern is partially deceptive, for "it relies on minimizing and delaying information from the user[132]", while hiding additional charges or costs until the user is close to finishing the transaction or the sign-up process[133]. This deceptive pattern takes full advantage of the sunk-cost fallacy, as since the user has already invested significant time on the platform (probably filling out the shipping/billing address form and, often, signing up), they are more likely to proceed, in spite of the surprise costs. The **hidden subscription** deceptive pattern acts in a similar fashion, but instead of operating on one-time purchases, it "charges users a recurring fee under the pretense of a one-time fee or a free trial[134]". As BRIGNULL explains, "once they have signed up, the service is usually covert and the user is sent no emails or notifications reminding them that they are paying on a recurring basis, so that payments continue for as long as possible[135]". As this pattern is usually combined with the hard to cancel one, the user ends up incurring in the payment of the fee due to either not realizing that there is an ongoing subscription, or due to being faced with too much work to cancel, as explained above.

Continuing this enumeration, we will proceed to the **sneaking** pattern, in which "the user is drawn into a transaction on false pretenses, because pertinent information is hidden or delayed from being presented to them[136]". This pattern preys on the default effect bias, for the user might either not notice an extra item added to their cart without their consent (or the option to remove it might be obscured) and thus, ends up conforming to the pre-selected product that is already there, going forward with the purchase, anyway. This pattern, according to the taxonomy we have been following, is considered, like the two previous ones, a partially deceptive one[137].

[131] MATHUR et al., op. cit., p. 21
[132] MATHUR et al., op. cit., p. 13
[133] Deceptive Patterns - types – Hidden Costs (n.d.).
[134] MATHUR et al., op. cit., p. 13
[135] Deceptive Patterns - types – Hidden subscription (n.d.).
[136] Deceptive Patterns - types – Sneaking (n.d.).
[137] Mathur et al., op. cit., p. 13.

The **nagging** deceptive pattern refers to a resource depletion tactic[138] in which the user is constantly interrupted with requests to take a specific action, which "depletes the user's time and attention" to the point where they might feel like it is easier to consent (forcefully, due to exhaustion) to what the platform wants them do accept, even if it is not on the user's best interest. We consider this pattern to be asymmetric, for the user really is given no other choice but to conform to the platform's wishes (other than being constantly nagged by requests).

The **preselection** pattern is quite self-explanatory. As "people tend to go with the option that is already chosen for them, even if there are other choices available[139]", this pattern exploit this phenomenon (the defaut effect bias), which means that unless a user notices the preselection (and understands what it means), they might end up coerced into accepting terms they otherwise would not. We consider this pattern to be asymmetrical, for the fact that there is a knowledge imbalance between user and platform.

The **trick wording** and the **visual interference** patterns subvert and exploit the psychology behind the basic principles of design, which we explained above. On the one hand, users have an expectation of what they will find on a website (both text and content-wise), and on the other, they usually scan through most of the information which they are presented with, as there are far too many things happening, at the same time, all the time. So, on both these deceptive patterns, "the user is misled into taking action, due to the presentation of confusing or misleading language[140]", on first case, or their expectations in regards to the contents on the page are frustrated because they are "hidden, obscured or disguised[141]", on the second one. The trick wording pattern can be categorized as asymmetrical and covert, and preys on the framing and default biases[142].

In the case of visual interference, the most common way to subvert the user's expectation is to present important information either in a lower contrast or in smaller text (or, also, forcing the user to scroll further down the page in order to find the relevant information)[143].This pattern exploits both the anchoring and framing biases, and is asymmetrical, covert and, at the very least, partially deceptive[144].

[138] Deceptive Patterns - types – Nagging (n.d.).
[139] Deceptive Patterns - types – Preselection (n.d.).
[140] Deceptive Patterns - types – Trick Wording (n.d.).
[141] Deceptive Patterns - types – Visual Interference(n.d.).
[142] MATHUR et al., op. cit., p. 12
[143] Deceptive Patterns - types – Visual Interference (n.d.)
[144] MATHUR et al., ibid

DECEPTIVE DESIGN PATTERNS

As noted by HILDEBRANDT, in the digital world, reconfiguring choice architectures in interfaces and platforms is a power and is precisely through it that digital companies can force customers to accept undesirable data processing conditions in exchange for access to a particular digital platform in which they are 'locked- in[145]', thus reinforcing already pre-existent inequalities and impairing user autonomy and free choice. So, as MALGIERI states, in online platforms, there is no need to force users to give their consent to data processing – it is enough that the architecture nudges us to act the way they wish us to[146].

Albeit deceptive patterns might have different nomenclatures and categories, as we described, they stand for the same thing: tactics used to manipulate the user into making decisions they originally did not want to do; thus, contending with their autonomy. In our opinion, however, there are advantages in focusing on the manipulative tactics themselves rather than on the ends[147].

Over the course of the years, several scholars from different fields, such as behavioral economics (who refer to them as *sludge*[148]), UX and UI design (who have been using the term *dark patterns*[149]), and law (who refer to these tactics merely as *market manipulation*[150] [151]), have been delving into this theme, but only in the last couple years has it been garnering the attention it deserves[152]; although under a plethora of different

[145] SAX, M. (2021). Between empowerment and manipulation: The ethics and regulation of for-profit health apps. In Wolters Kluwer. https://pure.uva.nl/ws/files/58919538/Thesis.pdf, as cited by Malgieri, G. (2023), op. cit., p 52.
[146] MALGIEIRI, G. (2023), Vulnerability and Data Protection Law. In Oxford University Press eBooks. https://doi.org/10.1093/oso/9780192870339.001.0001, pp. 53-54.
[147] Accordingly, LUGURI, J.B. and STRAHILEVITZ, L. (2021) "Shining a Light on Dark Patterns," Journal of Legal Analysis, 13(1), pp. 43–109, p. 52. Available at: https://doi.org/10.1093/jla/laaa006. BRIGNULL, H. Deceptive Patterns, EDPB, Guidelines 02/2023.
[148] THALER, R. H., (2018), "Nudge, not sludge", Science, Vol. 361, Issue 6401, pp.431-431. Available at: DOI: 10.1126/science.aau9241
[149] BRIGNULL, H. (2010), https://www.deceptive.design
[150] HANSON, J.D. and KYSAR, D.A. (1999) "Taking Behavioralism seriously: Some evidence of market manipulation," Harvard Law Review, 112(7), 630-745,. Available at: https://doi.org/10.2307/1342413.
[151] CALO, R. (2014) "Digital market manipulation", George Washington Law Review, Vol. 82., pp. 995-1051, p. 1003, Available at: https://digitalcommons.law.uw.edu/faculty-articles/25/,
[152] Beyond the previously mentioned website (www.deceptive.design), several pages on social media have also been trying to bring the existence of these patterns to our attention. For example, the Twitter page @assholedesign (https://twitter.com/AssholeDesign), or reddit's subreddit r/assholedesign (https://www.reddit.com/r/assholedesign)

nomenclatures. Evidence of such is the number of studies finding their existence in a widespread way among many websites and services[153] [154] [155].

We need to mention that, recently, LEISER and SANTOS have developed a "spectrum of visibility of deceptive patterns[156]". According to these authors, deceptive patterns can be divided into visible patterns, darker and darkest patterns, referring to the detectability of each tactic[157]. The same authors identify and develop, beyond the deceptive patterns we had the chance to analyse, algorithm-based deceptive patterns and AI-based deceptive patterns, which are much more difficult to detect, given how they are built-in the system. Irrespective of the importance and relevance of this matter (as it poses an even greater regulatory challenge), we will not be delving into this theme in our dissertation, as it goes beyond its scope.

[153] MATHUR, A. et al. (2019) op. cit. p. 2

[154] European Commission, Directorate-General for Justice and Consumers, LUPIÁÑEZ-VILLANUEVA, F., BOLUDA, A., BOGLIACINO, F. (2022). Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report, Publications Office of the European Union, p. 6, https://data.europa.eu/doi/10.2838/859030

[155] DI GERONIMO, L. et al. (2020) UI dark patterns and where to find them, p. 5 Available at: https://doi.org/10.1145/3313831.3376600.

[156] Brignull, H. (2023), op. cit., p. 231

[157] SANTOS, C., & LEISER, M. (2024). View of Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface. European Journal of Law and Technology, 15(1), https://ejlt.org/index.php/ejlt/article/view/990. https://ejlt.org/index.php/ejlt/article/view/990/1084, p. 6

VULNERABILITY

Concept

Vulnerability can be described as the "significant likelihood of incurring identifiable harms while lacking the ability to protect oneself[158]" in their autonomy, dignity, and integrity[159]. It is quite difficult, if not outright impossible, to find a single definition for harm, given the plethora of meanings it can have depending on the context[160]. So, and according to MALGIERI, whose opinion we closely follow, we propose that "harm should mean, at least, a legal or similarly significant effect[161]" on data subjects' fundamental rights.

Vulnerability has, too, been depicted as "a heuristic device that permits analyzing hidden assumptions and biases folded into legal practices[162]". This means that, only after accepting the universal character of human vulnerability, it is possible to properly achieve social justice through the adaptation of the existent institutions[163] because to be vulnerable an inevitable part of human condition due to the nature of our existence[164][165], even if some people are more vulnerable than others, or more vulnerable in certain situations and not in others.

Indeed, LUNA not only states that vulnerability can pertain to a series of factors (such as lack of power and possibility of exploitation and inability to properly evaluate risks and harms in proposals[166]), but has also developed the theory of layered

[158] MALGIERI, G. (2023), Op. cit., p. 73
[159] MACKENZIE, C., ROGERS, W., & DODDS, S. (2014). Introduction: what is vulnerability and why does it matter for moral theory? In C. Mackenzie, W. Rogers, & S. Dodds (Eds.), Vulnerability: new essays in ethics and feminist philosophy (pp. 1-29). Oxford University Press.) 4– 5.
[160] MALGIERI, G. (2023), Op. Cit., p. 74
[161] Ibid.
[162] FINEMAN, M. A. (2008) "The Vulnerable Subject: Anchoring Equality in the Human Condition', Yale Journal of Law and Feminism 23; MA Fineman, 'Vulnerability and Social Justice' [2019] SSRN Electronic Journal <https:// www.ssrn.com/ abstr act= 3352 825, as cited by MALGIERI, G. (2023), ibid.
[163] FINEMAN, M. A. (2019). *Vulnerability and social justice*. Emory Law Scholarly Commons. https://scholarlycommons.law.emory.edu/faculty-articles/116/, 314-369, p. 369
[164] ROGERS, W., MACKENZIE, N., & DODDS, N. (2012). Why bioethics needs a concept of vulnerability. International Journal of Feminist Approaches to Bioethics, 5(2), 11-38, https://doi.org/10.2979/intjfemappbio.5.2.11, p. 12.
[165] MACINTYRE, A. C. (2001). Animales racionales y dependientes: Por qué los seres humanos necesitamos las virtudes, PP. 102-103, as cited by MASFERRER, A., & GARCÍA-SÁNCHEZ, E. (2016). Vulnerability and human dignity in the age of rights. In Ius gentium (pp. 1–25). https://doi.org/10.1007/978-3-319-32693-1_1, p. 2.
[166] LUNA, F. (2018). Identifying and evaluating layers of vulnerability – a way forward. Developing World Bioethics, 19(2), 86–95. https://doi.org/10.1111/dewb.12206, p. 89

vulnerability, to which we adhere to, despite the criticisms faced[167]. According to this author, "being vulnerable reveals that a person might be exploited under certain circumstances[168]" but not on others, or not always[169]. As MALGIERI explains it, this theory makes vulnerability context-dependent[170]. As stated by the same author, vulnerability is universal, but "such a condition of weakness and marginalization may vary from one individual to another; it may have different degrees of severity and many different factors[171]". In sum, we agree with the aforementioned authors, and will treat vulnerability as a condition inherent to all human beings, although in different degrees and variable from one individual to another. Thus, the intensity of legal protection needs to be proportional to the degree of vulnerability of each person[172].

Vulnerable persons in the jurisprudence

Although the European Court of Human Rights recognizes that certain groups are vulnerable and need special protection (lack of maturity, mental disability, and state of dependency), it is yet to develop a notion of vulnerability when it concerns to private life, privacy, or data protection, as prescribed by Article 8 of the Charter. The first decision of the European Court of Human Rights (hereinafter, ECHR) in which the idea that the more vulnerable persons should be protected was Dudgeons v. UK[173].

[167] Namely, some authors consider this theory to be too inclusive and therefore, render everyone vulnerable, such as LEVINE, but we do not think that is the case – as we explored on the first chapter, everyone can incur in cognitive biases and bounds, for example.
[168] LUNA, F. (2018), op. Cit., p. 91
[169] See, also, BAKER, S. M., GENTRY, J. W., & RITTENBURG, T. L. (2005). Building Understanding of the Domain of Consumer Vulnerability. Journal of Macromarketing, 25(2), 128-139, https://doi.org/10.1177/0276146705280622, p. 137, who state that "although some classes of people are more likely to experience vulnerability, that does not mean that people in those classes are always vulnerable."
[170] MALGIEIRI, G. (2023), op. cit., p. 51
[171] LUNA, F. (2009). Elucidating the Concept of Vulnerability: Layers Not Labels. International Journal of Feminist Approaches to Bioethics, 2(1), 121–139. http://www.jstor.org/stable/40339200, as cited by MALGIEIRI, G. (2023), ibid.
[172] MALGIERI, G. (2023), Op. cit., p. 51
[173] Dudgeons v. UK, (22.10.1981), Application 7525/76 in which "the court recognizes that one of the purposes of the legislation is to afford safeguards for vulnerable members of society".

Eventually, the ECHR expanded the notion of vulnerability to politically and socially disadvantaged groups[174], to asylum seekers[175], people living with HIV[176] or with terminally ill diseases[177] and individuals living in poverty[178] [179], which confirms that the ECHR's view of vulnerable persons is quite subjective. As noted by MALGIERI, "the Court sees vulnerability as relational, harm-based[180]" and dependent on the circumstances of each specific case. In all of the aforementioned decisions, though, the ECHR has decided that vulnerability needs to be addressed by each State through the implementation of positive measures specific to each situation.

Over time, the concept of vulnerability has gradually emerged in various legal contexts, such as employment law to biomedical research, and from migration policy to social assistance[181].In the cited author's view, the fragmented way vulnerability is presented as translates the fact that it is a "contextual, relative and relational[182]" concept, with which we agree, given the theory of layered vulnerability which we previously mentioned. Vulnerability, in itself, can have different degrees both in duration (temporary or permanent) and in kind (we can talk about physical or mental vulnerability). It is the intersection of each of these points, in a specific context, that constitute the layers of vulnerability to which LUNA refers to on her works. As stated, these layers "can be of different relevance and importance, temporary or permanent, physiological or pathological. The intersection of these layers in a given structural and relational context qualifies a data subject's vulnerability level[183].

The vulnerable data subject – the bridge between vulnerability in consumer law to privacy

To define who the vulnerable data subject is, we must delineate the average data subject. The GDPR's definition of data subject is made indirectly, through the definition of

[174] Chapman v.UK, Application 27238/95 (18.01.2001)
[175] M.S.S. v Belgium and Greece, (21.01.2011), Application 30696/ 09, Ilias and Ahmed v. Hungary (21.11.2019), Application 47287/15 and Z.A. and Others v. Russia (21.11.2019), Applications 61411/15, 61420/15, 61427/15 and 3028/16.
[176] Kiyutin v Russia (10.03.2011), Application 2700/ 10
[177] Pretty v. UK (29.04.2002), Application 2346/02, Popshvili v. Belgium (13.12.2016), Application 41738/10.
[178] Airey v. Ireland (9.10.1079), Application 6289/73
[179] Yordanova v. Bulgaria, (05.06.2012), Application 25446/ 06
[180] MALGIERI, G. (2023), op. Cit., p. 59.
[181] MALGIERI, G. (2023), op. Cit., p. 59.
[182] Ibid.
[183] MALGIERI, G. (2023), op. Cit., p. 55.

'personal data', from which we can infer that the data subject is an identified or identifiable natural person, to whom some data must be related to. This notion is universal, as we can conclude from the fact that multiple legal texts consecrate the processing of personal data a fundamental right, such as the Charter of Fundamental Rights of the European Union[184] (hereinafter, the Charter) and the Treaty on the Functioning of the European Union (hereinafter, TFUE), pursuant to which everyone is recognized the right to the protection of personal data concerning them[185], and dynamic, particularly where it concerns the identification vs. identifiability debate, discussed by MALGIERI, as a person might not be identifiable from the standpoint of one controller or at a certain moment, but might be on another moment in time or from the perspective of another controller[186].

As the same author argues, and whom we closely follow, the data subject may only be one person, legally, but their particular characteristics (legal status, mental condition, level of awareness and understanding of data protection risks and rights, the likelihood of being at risk in their fundamental rights, resilience, or reaction to such risks) should be relevant and accounted for in the data protection framework[187], the same way that it is accounted for in consumer law, as we concluded, previously, that those characteristics can render individuals vulnerable, and that they can be present in everyone.

It is true that the GDPR's structure does not acknowledge, directly, an average data subject, but it is implied, especially due to the proximity of rationale existent between consumer and privacy law. As FUSTER notes, "the depiction of data subjects as consumers is sometimes put forward to promote the need to reinforce the protection of users of online platforms, notably by resorting to safeguards and notions borrowed from consumer law[188]".

Accordingly, we can look at Recital 18 of the Unfair Commercial Practices Directive, which defines the average consumer as someone who is *reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural,*

[184] Charter of Fundamental Rights of the European Union, Article 8.
[185] TFUE, Article 16.
[186] KOOPS, B. (2014). The trouble with European data protection law. International Data Privacy Law, 4(4), 250–261. https://doi.org/10.1093/idpl/ipu02, p. 250, as cited by MALGIERI, G. (2023), *Op. Cit.*, p. 24.
[187] MALGIERI, G. (2023); Op. Cit., p. 27.
[188] FUSTER, G. G. (2014). How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection. IDP Revista De Internet Derecho Y Política, 92-104, P. 99, https://doi.org/10.7238/idp.v0i19.2424

and linguistic factors, as interpreted by the Court of Justice[189] [190]. As we could see on the first chapter, however, we do not always behave rationally and are susceptible to incurring in cognitive biases, so it is for good reason that this protection is warranted, especially with the use of deceptive design patterns.

The same recital we cited above states that *where a commercial practice is specifically aimed at a particular group of consumers, such as children, it is desirable that the impact of the commercial practice be assessed from the perspective of the average member in that group*, and proceeds to state, on Recital 19, that *additional protection may be necessary when the consumer has certain characteristics (such as age, physical or mental infirmity or credulity).* In this field of law, the protection of the consumer – be it the average or the vulnerable one – comes from the fact that, generally, the consumer is the weaker party when before a professional, due to the power imbalance generated by information asymmetries[191], thus confirming the fact that there is a relational element in consumer vulnerability deriving from both internal factors such as a person's sensitivity or on external factors, such as the massive amount of data a controller can gather, in the case of data protection, for example[192].

In the same direction, the European Commission Report of 2016 confirmed the fact that vulnerability "is best viewed as a spectrum[193]", as it is not static. It is also worth noting that this report also recognizes that a great part of consumers in the EU face significant "difficulty in obtaining or assimilating information (regarding information asymmetry, and a higher susceptibility to marketing practices[194]", among others.

Additionally, we can find that in the recent Guidelines for the implementation of the UCPD, the Commission recognizes, explicitly, the existence of multi-dimensional

[189] For example, see the interpretation of the CJEU in Case C-210-96, Gut Springenheide and Tusky (1998), https://curia.europa.eu/juris/liste.jsf?num=C-210/96, Case C-220/98, Estée Lauder Cosmetics GmbH & Co. OHG v. Lancaster Group GmbH (2000), https://curia.europa.eu/juris/liste.jsf?language=en&num=c-220/98, Case C-470/93, Verein gegen Unwesen in Handel und Gewerbe Köln e.V. v. Mars GmbH (1995), https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=ecli:ECLI:EU:C:1995:224, and Case C-122/10, Konsumentombudsmannen v. Ving Sverige AB (2011), https://curia.europa.eu/juris/liste.jsf?language=en&num=C-122/10 .

[190] For example, in C-210/96, Gut Springenheid v. Tusky (16.07.1998), in which the court considers the consumer to be reasonably well-informed, observant and circumspect.

[191] MALGIERI, G. (2023), Op. Cit., p. 34.

[192] MALGIERI, G. (2023), Op. Cit., p. 69.

[193] Consumer Vulnerability Across Key Markets in the European Union, (January 2016). Available on: https://commission.europa.eu/system/files/2018-04/consumers-approved-report_en.pdf , p. 39

[194] Ibid, p. 44-48

forms of vulnerability which are particularly concerning in the digital environment[195], as we will analyze on the following chapter.

As noticed by MALGIERI, the nature of consumer vulnerability is even more evident when microtargeting and data mining contribute to further the aforementioned information asymmetry existent between consumer and data controller, resulting in greater power imbalance that is used to exploit these vulnerabilities[196].

We will, thus, adopt the definition of vulnerable consumer that the Commission proposes, and thus, a consumer will be deemed vulnerable if they, as a result of socio-demographic and behavioral characteristics, personal situation or market environment is at a higher risk of experiencing negative outcomes in the market, has limited ability to maximize their well-being, has difficulty in obtaining or assimilating information, is less able to buy, choose or access suitable products or is more susceptible to certain marketing practices[197].

When it comes to categorizing vulnerable consumers, we will follow the same reasoning we did for categorizing deceptive patterns and focus on the way their vulnerabilities show, in practice, therefore following the taxonomy with CARTWRIGHT proposes, especially as we can link them to vulnerability drivers. Therefore, we can identify informational vulnerability, pressure vulnerability, supply vulnerability, redress vulnerability, and impact vulnerability[198]. All of these vulnerabilities can be exploited through vulnerability drivers, such as deceptive design patterns, in our opinion. We will further develop this idea on the next subsection.

Lastly, even if the GDPR does not expressly mention a vulnerable data subject, we can find an opening for interpretation when we look at Recital 75, about the relevant risks to assess when conducting a DPIA (Data Protection Impact Assessment), where it

---

[195] Guidelines for implementing the UCPD (2021). Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XorC1229(05), p. 87

[196] MALGIERI, G. (2023), op. cit., p 69

[197] Consumer Vulnerability Across Key Markets in the European Union (Executive Summary), January 2016, p.

[198] CARTWRIGHT, P. (2015), Understanding and protecting vulnerable financial consumers, Journal of Consumer Policy, 38, 119-138, ISSN 1573-0700, as cited in Consumer Vulnerability Across Key Markets in the European Union, p. 45-46. Information vulnerability pertains to "situations where service providers have syperior information to some groups of consumers and use this to their advantage", supply vulnerability concerns "situations where a particular consumer group cannot participate in a market" due to external conditions, redress vulnerability happens when a particular group of consumers faces "particular difficulties in obtaining redress", pressure vulnerability refers to the cases where consumers are subjected to pressure from the seller, and, lastly, impact vulnerability refers to situations where certain consumer groups suffer greater loss due to their decisions than others and surges as a consequence of another source of vulnerability.

reads that *"where personal data of vulnerable natural persons, in particular of children, are processed"* there must be additional care. Despite the fact that the GDPR only specifically addresses children as vulnerable data subjects, the use of the expression *in particular* leads us to believe that not only other vulnerable subjects can be protected under this legal document, but also that they need equal protection for they have similar risks[199], as MALGIERI and NIKLAS note. On another important note, as theWP29 specifies, even if only children are expressly considered vulnerable, the concept of data subject is "universal and unique[200]", as explained above. The reason why children are more protected than other users is because of their lack of awareness of the risks and consequences regarding their data, as recitals 38 and 58 of the GDPR explain. So, in line with what MALGIERI and NIKLAS defend, as well with what has been said by WP29, we are of the opinion that vulnerability cannot be limited only to children[201], for the reasons we explained above, as the key factor here is the existence of a significant power imbalance between the data subject and the data controller that is exacerbated by the use of deceptive design patterns in online platforms.

In conclusion, as far as we are concerned, there is no plausible reason not to extend these concepts and conclusions to the field of data protection and, therefore, to build both an average date subject and a vulnerable one. We will consider, for the purposes of this dissertation, as an average data subject, a subject who is as rational and well-informed as the average consumer, and capable of making autonomous decisions regarding their data[202]. If this were not the case, it would make no sense to establish consent, or to consecrate the conditions for it to be valid, as a legal basis for processing personal data[203], nor to establish transparent information duties[204] that must be fulfilled by the controller, because there would be no necessity to inform someone who could not decide.

Much like it happens in the field of consumer law, the theoretical average data subject differs from the real one. As several authors have emphasized, users do not behave rationally especially when it concerns their personal data[205] [206], which is a phenomenon

[199] Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. Computer Law & Security Review, 37, 105415. https://doi.org/10.1016/j.clsr.2020.105415, p. 8
[200] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, pp. 21-22.
[201] MALGIERI, G. and NIKLAS, J. (2020), *op. cit.*, p. 8
[202] MALGIERI, G. (2023), Op. Cit., pp. 35-40
[203] GDRP, Article 6, 1(a) and Article 7.
[204] GDPR, Articles 12-14.
[205] See, for example, REYNA, A. (2018), Op. Cit., or FUSTER, G.G. (2014), who also notes this phenomenon.
[206] Special Eurobarometer 359 (2011), Microsoft Word - Report EB 743 eid JUST JRC_EN Full report - final.doc (europa.eu), p. 54

that has been referred to as privacy-paradox[207]. This lack of rationality happens because biases can influence privacy choices in various ways, as the decisions users make in regards their personal data are context-dependent and shaped by both internal factors, such as emotions, cognitive biases and limited rationality, and by external factors, which involve transaction costs, framing, and the circumstances surrounding the choice, such as a company's privacy reputation and how privacy policies are presented[208]. Obviously, using deceptive design patterns only exacerbates this already existent issue, especially when users do not seem to read the privacy notices and policies presented to them[209], nor change the default privacy settings because they trust websites and companies to set the appropriate privacy options or lack the knowledge to[210].

MALGIERI explains that there are two different moments, in data protection, in which a user is more susceptible to suffering harms and, therefore, being vulnerable: during the data processing itself, and as a consequence of that data processing[211]. On the first moment, as the same author elucidates and building from what we explored above, the fact that a user is unable to understand or read the privacy policies (due to the existence of deceptive design patterns, for example), will negatively impact their exercise of their privacy rights[212]. Due to this, the second moment emerges: as a consequence of that lack of consent or inability to properly understand and control their choices, a user might share more data than intended, for purposes they do not acknowledge and might even result in discrimination, as "data-driven systems can serve as tools of potential discrimination and manipulation that may lead to physical and psychological harms[213]" as we will develop on the next subsection.

There is a deep connection between the concepts of human dignity and vulnerability, as shown by MASFERRER and GARCÍA-SÁNCHEZ, for the concept of human

[207] BARTH, S., and JONG., M. D.T., "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review" (2017), 34 Telematics and Informatics, as cited by Reyna (2018), Op. Cit., p. 6

[208] BORGESIUS, F. Z., "Behavioural Sciences and the Regulation of Privacy on the Internet" in Alberto Alemanno and Anne-Lise Sibony (eds.), Nudge and the Law. A European perspective, (Hart Publishing 2015), p. 197, as cited by REYNA (2018), Ibid.

[209] Publications Office of the European Union. (2019). *The General Data Protection Regulation : report.* Publications Office of the EU. https://op.europa.eu/pt/publication-detail/-/publication/87d359d4-a83c-11e9-9d01-01aa75ed71a1, p. 3. Only 13% of the respondents read the privacy statements, and, of 87% who do not read, 66% claim to not do so due to the length of the statement. Additionally, 31% find the statement unclear and difficult to understand.

[210] Ibid., p. 69.

[211] MALGIEIRI, G. (2023), op. cit., p. 80.

[212] Ibid.

[213] MALGIEIRI, G. (2023), op. cit., p. 81

dignity is built, in great part, on the idea that the most vulnerable individuals need protection[214]. In turn, human dignity is the basis for the right to privacy[215], as the latter is built on the free development of personality through the self-determination and self-flourishment of the individual[216]. Considering this connection, it makes even more sense to protect the most vulnerable individuals, as a dignity-based approach to data protection demands us to consider the specific needs and situation of vulnerable data subjects[217].

It is also worth noting that most of the existing guidelines protecting vulnerable groups focus on issues of informed consent and participation, highlighting problems of autonomy and integrity[218], as we could see. When it comes to privacy, human vulnerability cannot be ignored, especially with the rise of the deceptive patterns on the digital environment and how they can effectively potentialize an already existent vulnerability in the context of decision-making, autonomy, and consent, as the proposed Data Act has highlighted in recital 34[219]. That is also partially why we are not surprised when CALO states that "most cases of undue influence involve victims who lack capacity[220]".

In conclusion, any data subject can be vulnerable depending on a myriad of factors, and, they key-factor in assessing that vulnerability is the inherent power imbalance existent between subject and controller[221].

[214] MASFERRER, A., & GARCÍA-SÁNCHEZ, E. (2016). Vulnerability and human dignity in the age of rights. In Ius gentium (pp. 1–25). https://doi.org/10.1007/978-3-319-32693-1_1, p. 5.
[215] FLORIDI, L. (2016). On human dignity as a foundation for the right to privacy. Philosophy & Technology, 29(4), 307–312. https://doi.org/10.1007/s13347-016-0220-8, p. 307.
[216] VAN DEL SLOOT, B., (2014) 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen
Privacy Protection in the Age of Big Data?', Journal of Intellectual Property, Information Technology and Electronic Commerce Law, as cited by MALGIERI, G. (2023), op. cit., pp. 56-57
[217] MALGIERI, G. (2023), op. Cit., p. 57.
[218] MALGIERI, G. and NIKLAS, J., (2020), *op. cit.*, ibid.
[219] (Dark patterns) "can be used to persuade users, particularly vulnerable consumers, to engage in unwanted behaviors, and to deceive users by nudging them into decisions on data disclosure transactions or to unreasonably bias the decision-making of the users of the service, in a way that subverts and impairs their autonomy, decision-making and choice."
[220] CALO, R. (2017), op. cit., p. 592
[221] MALGIERI, G. (2023), op. cit., p.98

THE IMPACT OF DECEPTIVE PATTERNS ON VULNERABLE DATA SUBJECTS (Harms and consequences of vulnerability enhanced by Deceptive design patterns)

We can look and address the consequences of vulnerability from two standpoints: the first one regards finding remedies for the harms suffered by individuals, such as manipulation, or limitations to their autonomy caused by power imbalance[222], and the second one focuses on empowering individuals by giving them tools and safeguards so that they can overcome their vulnerable state[223], in addition to the two moments in which we explained above that the data subject is more vulnerable in, due to a plethora of factors, including cognitive biases exploited by deceptive patterns. We also adopted MALGIERI'S notion of vulnerability, thus describing it as the significant likelihood of incurring identifiable harm to a subject's fundamental rights and freedoms, so, it is the moment to conceptualize the harms that can occur, especially due to the use of deceptive design patterns on interfaces. We will start this subsection by stating that we consider deceptive design patterns to be a vulnerability driver.

Vulnerability drivers are a source of vulnerability, which means that they consist of "mechanisms through which consumers can become vulnerable and through which their vulnerabilities can be exploited[224]", either through specific means, such as through the inclusion of deceptive design patterns on the platforms, or through "wider contextual factors that can impact vulnerability too, such as social, economic, technical, political, geographical, and institutional factors that directly or indirectly influence the level of vulnerability of individuals[225]". Indeed, not only do deceptive patterns cause individual harms (such as privacy, financial and time loss, psychological harms and loss of freedom to think and make free, autonomous choices[226]), they also cause significant harm to specific groups of people that can also be considered vulnerable, such as people who suffer from time poverty, people with low education levels, people with low income, second language learners, people with cognitive impairments or disabilities, young and old people and also enhance the contextual vulnerability in which we sometimes can be

[222] LUNA, F. (2009). Elucidating the Concept of Vulnerability: Layers Not Labels. International Journal of Feminist Approaches to Bioethics, 2(1), 121–139. http://www.jstor.org/stable/40339200, as cited by MALGIEIRI, G. (2023), op. cit., p. 55.
[223] MALGIERI, G. (2023), Op. Cit., p. 50
[224] Ibid., p. 50
[225] MALGIERI, G. (2023), Op. Cit., p. 72
[226] BRIGNULL, H. (2023), op. cit., p. 167-170

(as the author exemplifies, if we do not sleep well at night, we will have more difficulty concentrating)[227] and we will be more susceptible to incur in biases and be manipulated. SANTOS et al. highlight, too, as harms caused by deceptive patterns, emotional load and social injustice[228].

The patterns we described on the first chapter can, thus, impair the ability to understand information properly about data processing, as well as the risks and significance of said processing, which not only results in the invalidity of the given consent, but also in the lack of power to properly exercise their personal data protection rights[229]. Therefore, the fundamental rights of autonomy, dignity and self-determination are put at stake, considerably, by these patterns, especially as they are growing in presence on websites[230].

We can thus state that there can be three elements that act as vulnerability factors: the data subject's characteristics, the controller's characteristics and power, and deceptive patterns, as a vulnerability driver[231].

With the usage of these tactics made specifically to lead users into making unintended choices and potentially harmful decisions, vulnerable users are put in an even more disadvantageous positions for they may not have the proper discernment to avoid these predatory tactics and, ultimately, find their data protection rights utterly violated, for the lack of understanding of their data protection rights and/or privacy notices will lead to a coerced consent[232] which, as we will see, is not valid.

To an extent, all deceptive patterns can have a severe impact on the user's autonomy and ability to consent. We consider, though, that the ones which affect this dimension further are the confirmshaming, comparison prevention, visual interference, and fake social proof ones. As SANTOS et al. highlight, all of these can limit users' agency as they both override their goals with the presentation of other information or make them look at the product "less critically[233]". When it comes to the loss of privacy, although related to loss of autonomy, we also agree with the previously cited author, who considers particularly problematic the nagging, obstruction, and default option patterns, along with

[227] BRIGNULL, H. (2023), op. cit., pp. 171-173.
[228] SANTOS, C. et al. (2024). Op. cit., p. 2.
[229] MALGIERI, G. (2023), Op. Cit., p. 166.
[230] Consumer Protection: manipulative online practices found on 148 out of 399 online shops screened (30.01.2023) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.
[231] MALGIERI, G. (2023), Op. Cit., p. 177
[232] MALGIERI, G. (2023), Op. Cit., p. 82
[233] SANTOS et al. (2024), op. cit., p. 7

the forced action ones[234]. The fact that users share more data than intended due to the use of these tactics can "lead to more extensive processing about user's behavior, preferences and attitudes and, ultimately, unwanted targeted advertising or profiling[235]".

When it comes to psychological harms, it is without surprise that we conclude that, after being exposed to deceptive patterns, users experience emotional distress, addiction, cognitive burden, and attentional harms[236].

When it comes to quantifying the effect of deceptive patterns, the studies conducted by LUGURI AND STRAHILEVITZ in 2021 are of utmost importance to show the effect that the usage of deceptive patterns have on users. These studies presented two key findings: one, dark patterns are effective in manipulating consumer choice (and that mild patterns are more dangerous, as they do not generate as much — if any at all! — backlash as opposed to when aggressive patterns are employed) and two, some patterns are more effective than others.

This study also showed that less educated individuals are more likely to be affected by deceptive patterns[237], which goes hand in hand with an European experiment on decision-making, conducted on six Member States (Bulgaria, Germany, Italy, Poland, Spain and Sweden) that concluded the same thing: both older and less-educated people are more likely to make inconsistent choices when confronted with deceptive patterns[238].

Another experiment conducted in Europe (specifically, in Spain, Germany and Italy) to analyze consumers' neurological responses has showed the same, highlighting that the "forced action combined with personalization not only hampered the extent to which participants could successful complete a common day-to-day task online, but also increased their heart rate when dealing with the pop-up feature[239]". The two main conclusions are that consumers have both grown used to the presence of these tactics on the digital world, and that, maybe because of this habituation, the neurological response is not sufficiently relevant. Still, we believe that just the fact that people have grown familiar with the usage of these tactics should be enough to warrant a legal response.

---

[234] Ibid., p. 8
[235] Ibid.
[236] Ibid., p. 9
[237] LUGURI, J.B. and STRAHILEVITZ, L. (2021) Op. cit., pp. 43–109. Available at: https://doi.org/10.1093/jla/laaa006.
[238] European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F. (2022). Op. cit., p. 6, https://data.europa.eu/doi/10.2838/859030
[239] Ibid.

In regards to cookies, BORBERG et al. have also highlighted that deceptive design patterns employed in the design of cookie notices makes users more likely to consent to data collection when they probably would not, if not these insidious tactics[240]. This study found that users suffering from time poverty, for example, were more susceptible to simply accepting the cookie consent dialog pop-up just so that they could access the website they needed, even if they were unhappy about that decision[241] since they would not have the time to read the entire notice and process the information it contained, as we previously mentioned. On the same line, UTZ et al. have also acknowledged that around 57.4% of cookie consent notices use deceptive patterns to "steer websites visitors towards accepting privacy-unfriendly options[242]".

So, to conclude this subsection, we will say that the legislator needs to adopt and consecrate adequate safeguards so as to ensure the fulfilment of vulnerable users' self-determination and self-flourishing and thus, their dignity as human beings[243].

[240] Borberg, I. M., Hougaard, R., Rafnsson, W., & Kulyk, O. (2022). "So I Sold My Soul": Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions, https://doi.org/10.14722/usec.2022.23026, p. 10

[241] Ibid, p. 11.

[242] UTZ, C. DEGELING, M., FAHL, S., SCHAUB, F., and HOLZ, T., (2019) (Un)informed Consent: Studying GDPR Consent Notices in the Field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212, P. 977

[243] MALGIERI, G. (2023), Op. Cit., p. 57

LEGAL REGULATION

On the first chapter, we discussed the concept of design and its underlying principles and psychology, to show how they can be twisted for deception by taking advantage heuristics and cognitive bounds and biases. Following, we delved into the definition and categorization of deceptive design patterns and introduced the way they are widely used online, how they cause substantial harm to users, and why measures must be taken in order to re-establish the balance between companies and users, particularly those who are vulnerable. On the second chapter, we introduced and conceptualized the notion of vulnerability in the field of data protection, and how deceptive design patterns prove to be more harmful to vulnerable individuals.

So, as legal regulation (and enforcement) is crucial in order to do so, on the present chapter we will focus on that aspect. It is important to note that most of the existing legislation concerning the protection of users against deceptive patterns regards consumer law and not privacy law, so we will inevitably have to focus on this field, too. It is also important, because while the concept of vulnerable consumer exists and has been largely discussed both by the scholars and in jurisprudence, the same has not happened to data subjects. As MALGIERI notes, "consumer law and data protection law cannot be considered as two separate monoliths[244]" because not only are the two fields similar in what they aim to protect, in the digital market and economy we currently live it, most consumers are also data subjects[245].

Therefore, we will start this chapter by making a comparative analysis of the US' legislation regarding the subject of our study and, afterwards, we believe it is necessary to analyze, extensively, the EU stance on the topic, as we believe it is important to compare the way the two legal systems work against the usage of deceptive design patterns. This will include looking into the relevant legal provisions, both enacted and proposed (in particular, the UCPD, the GDPR, DSA, DMA, Proposed AI Act and Proposed Data Act), into any existing soft law and into the existent case law of both the CJUE and domestic courts, and, possibly, into the fines applied by the administrative authorities. Afterwards, we will delve deeper into the governing principles of data

[244] MALGIERI, G. (2023). Vulnerability and Data Protection Law. In Oxford University Press eBooks. https://doi.org/10.1093/oso/9780192870339.001.0001, p. 30.
[245] FUSTER, G. G. (2014). How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection. IDP Revista De Internet Derecho Y Política, 19, 92. https://doi.org/10.7238/idp.v0i19.2424, p. 99, as cited by Malgieri, G. (2023), ibid.

protection, for we believe after arguing in the first section how they are affected by the usage of deceptive design patterns, it is important to further explain them and their dimensions, and that will be the bridge between the first part of the dissertation and the second part; in which we will study the concept of data subjects and argue about the existence of standard data subjects and vulnerable data subjects.

US Law

Firstly, we can highlight the Federal Trade Commission Act[246] (hereinafter, FTC Act), promoted by the Federal Trade Commission (hereinafter, FTC), which restricts the use of unfair or deceptive practices in commerce by defining such practices, preventing their deployment, and warranting monetary redress for conducting these harmful practices to consumers. Therefore, we must look at Section 5 of this act[247]. For these purposes, the FTC considers any "representation, omission or practice" that is material and likely to mislead consumers who are acting reasonably under the circumstances as deceptive[248]".

The materiality of the act can be translated into being one that is likely to affect consumer's choice or conduct regarding a product — it has to be important to the consumer, as noted by the cited policy statement[249]. This has been confirmed numerous times by the Courts[250] [251] [252].

Other federal laws that are worth mentioning are the Equal Credit Opportunity Act[253] (hereinafter, ECOA), the Children's Online Privacy Protection Act[254] (hereinafter,

[246] Federal Trade Commission Act (2006), Available for consultation at: https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act (Last Access: June 2023)
[247] § 45. Unfair methods of competition unlawful; prevention by Commission (Sec. 5)
(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful (...) (4)(A) For purposes of subsection (a) of this section, the term "unfair or deceptive acts or practices" includes such acts or practices involving foreign commerce that: cause or are likely to cause reasonably foreseeable injury within the United States; or involve material conduct occurring within the United States.
[248] FTC Policy Statement on Deception (1983), Appended to Cliffdale Associates, Inc. 103 F.T.C. 110, 174 (1984), p. 1, as cited by Luguri, J.B. and Strahilevitz, L. (2021), op. cit., p.83
[249] Ibid, p. 5
[250] See, for example: FTC v. Algoma Lumber Co., 291 U.S. 67 (1934), in which it was held by the Supreme Court that the advertised material (pinewood) had to match the sold one, in quality. That would be material information for the consumer.
[251] FTC v. Cyberspace.com, LLC
[252] FTC v. Williamson Tobacco Corp.
[253] The Equal Credit Opportunity Act., https://www.justice.gov/crt/equal-credit-opportunity-act-3
[254] Children's Online Privacy Protection Rule ("COPPA"), https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

COPPA), the Restore Online Shopper's Confidence Act[255] (hereinafter, ROSCA), the Controlling the Assault of Non-Solicited Pornography and Marketing Act[256] (hereinafter, CAN-SPAM), the Telemarketing Sales Rule[257] (TSR) and the Truth in Lending Act[258] (TLA). As noted by BRIGNULL, although most of these acts do not directly refer to deceptive patterns, they can cover against them[259]. The exception is found in the ROSCA, which specifically protects consumers against the hard to cancel pattern, specifically in its section 3. We also must highlight the COPPA, as it protects a category of vulnerable data subjects – children.

On a state level, there are many examples of legal texts prohibiting the use of deception. The California Privacy Rights Act[260] (hereinafter, CPRA) does specifically mention dark patterns in its text, and states that "agreement obtain through use of dark patterns does not constitute consent[261]" and that when a consumer can opt-in to consent, dark patterns must not be used to obtain said consent.

The Colorado Privacy Act[262] (hereinafter, CPA), the Connecticut Data Privacy Act[263] (hereinafter, CTDPA) and the Oregon Consumer Privacy Act[264] (hereinafter, OCPA) also specifically mention dark patterns as well, going in the same direction as the CPRA, both of them defining dark patterns in the same way and invalidating consent obtained through their use.

The New York General Business Law[265] (hereinafter, NY GBL), the Utah Consumer Privacy Act[266] (hereinafter, UCPA), the Massachusetts Consumer Protection Act[267] (hereinafter, MCPA) and the Washington Consumer Protection Act[268] (hereinafter,

---

[255] Restore Online Shoppers' Confidene Act (ROSCA), available for consultation here: https://www.ftc.gov/system/files/documents/statutes/restore-online-shoppers-confidence-act/online-shoppers-enrolled.pdf

[256] CAN-SPAM Act: A compliance guide for business. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business

[257] Telemarketing Sales rule. Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/telemarketing-sales-rule

[258] Truth in lending. (n.d.). OCC.gov. https://www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/truth-in-lending/index-truth-in-lending.html

[259] BRIGNULL, H., (2023), op. cit., pp. 200-201.

[260] Section 1798.140(h), California Privacy Rights Act. Dark patterns are defined as *means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation.*

[261] Ibid.

[262] Section 6-1-1303(6), Colorado Privacy Act

[263] Section 1(6) and (11), Connecticut Data Privacy Act.

[264] Section 646A-604, Oregon Consumer Privacy Act.

[265] Section 349, New York General Business Law

[266] Section 13-61-101, Utah Consumer Privacy Act.

[267] Section 2(a), Massachusetts Consumer Protection Act.

[268] RCW 19.86, Washington Consumer Protection Act

WCPA), along with the Virginia Consumer Data Protection Act[269] (VCDPA) do not specifically mention deceptive patterns, but they both do prohibit deceptive acts or practices while conducting a business.

On Texas, there is the Texas Deceptive Trade Practices – Consumer Protection Act (hereinafter, DTPA), which prohibits false, misleading, or deceptive acts or practices in the conduct of trade and commerce. This state's Business and Commerce code also prohibits these acts on Chapter 17[270].

As we stated before, the American courts have been considering the employment of deceptive patterns as unlawful, but they have refrained from naming them, until recently.

On April 9, 2019[271] the Deceptive Experiences to Online Users Reduction Act (DETOUR Act) was introduced which aimed to prohibit the usage of exploitative and deceptive design practices by large online operators in order to protect consumers[272]. Although it was not yet enacted, on August 12th, 2024, the Biden-Harris administration has launched the "Time is Money" initiative, which aims to "crack down on all the ways that corporations – through excessive paperwork, hold times, and general aggravation – add unnecessary headaches and hassles to people's days and degrade their quality of life[273]". This initiative also recognizes how these actions configure a deliberate choice from companies, who "design their business processes to be time-consuming or otherwise burdensome for consumers[274]" in order to maximize profit at the expense of people. Even though it seems to specifically aim certain deceptive patterns (like hard to cancel, hidden

[269] Section 59.1-571, Virginia Consumer Data Protection Act.
[270] Business And Commerce Code Chapter 17. Deceptive Trade Practices. Specifically, see the section 17.46 of this act.
[271] Deceptive Experiences To Online Users Reduction Act (DETOUR Act), Senate Bill 1084, 116th Congress, introduced April 9, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/1084/text
[272] Namely, the unlawfulness of designing, modifying or manipulating a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data, of segmentation consumers of online services into groups for the purposes of behavioral or psychological experiments or studies, except with the informed consent of each user involved; or of designing, modifying, or manipulate a user interface on a website or online service, or portion thereof, that is directed to an individual under the age of 13, with the purpose or substantial effect of cultivating compulsive usage, including video auto-play functions initiated without the consent of a user, prohibited by Section 3 of the DETOUR Act.
[273] House, W. (2024, August 13). FACT SHEET: Biden-Harris administration launches new effort to crack down on everyday headaches and hassles that waste Americans' time and money. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2024/08/12/fact-sheet-biden-harris-administration-launches-new-effort-to-crack-down-on-everyday-headaches-and-hassles-that-waste-americans-time-and-money/
[274] Ibid.

costs, hidden subscription, and obstruction), it represents a very important step towards the regulation of manipulative design in the US.

Among other measures, some of the key actions proposed involve facilitating the cancellation of subscriptions and memberships, requiring automatic cash refunds (in regards to airline companies), and ensuring that companies providing bad services are held accountable. This last one is particularly interesting as it originates from a proposal from the FTC that specifically aims the fake social proof deceptive pattern, as their goal is to not only impede the use of fake reviews and paid positive reviews, but also to keep companies from hiding honest negative reviews, as these "deceive consumers looking for real feedback on a product or service and undercut honest businesses[275]".

Case Law

As explained at the beginning of this chapter, we will now analyze some recent court decisions from the US' courts, as we are of the opinion that it is important to look at the way justice is tackling the use of deceptive design patterns. We will consider three decisions in this subsection: State of Texas vs. General Motors LLC (hereinafter,GM) and OnStar LLC, FTC v. Amazon.com and FTC v. Publishers Clearing House LLC.

On August 13th, 2024, the state of Texas has sued GM and OnStar LLC[276] for deceiving drivers, since 2015, into sharing detailed driving records from over 14 million of its vehicles, through the telematics system installed on said vehicles, effectively resulting in the deceptive collection of "scores of data points from consumers about their driving habits, monetized that data by selling it to other commercial actors and permitted those actors to use the ill-gotten data to make adverse decisions when dealing with those same consumers[277]". As if this was not enough, GM also sold customers' personally identifiable information[278].

The data collected by GM included, among other factors, the date and time, the speed at which the vehicle circulated, whether or not passengers and the driver wore seatbelts, and distance driven, which then it sold to other companies to calculate a customer driving score based on risk factors such as late-night driving, instances of sharp

[275] Ibid.
[276] State of Texas v. General Motors LLC & OnStar LLC, available for consultation here: https://www.texasattorneygeneral.gov/sites/default/files/images/press/General%20Motors%20Data%20Privacy%20Petition%20Filed.pdf
[277] State of Texas v. GM & Onstar, p. 2
[278] Ibid., p. 26

turns and hard braking, hard acceleration events and driving over 80 miles per hour[279]. In turn, this data was sold to insurance companies, who then used these scores to assess the risk of clients, both current and future. As highlighted, this resulted on higher premium prices and dropped coverage for their insured parties, and in coverage denials for clients[280].

Even though GM claimed that their clients consented to the collection, use and selling of their data, it was proven that such consent could not be deemed valid for it was obtained through the use of "several false, misleading and deceptive techniques (…) including through its utilization of an aggressive onboarding program that included misrepresenting to customers that its dealership onboarding process was a pre-requisite to taking ownership of their vehicles[281]" In regards to their privacy practices, GM also severely violated its customers rights, for their policy was extensive and made use of "confusing privacy statements[282]" so as to obscure their concrete goal and make sure that their abusive terms would be accepted.

Through the petition, it is clear that GM made use of several deceptive patterns in order to manipulate their customers: first, they were essentially forced into enrolling GM's connected vehicle services (which appeared to be mandatory, but was a "deceptively designed sales flow[283]"), under the pretense of it being for better entertainment, safety, and control, which resulted in clients unsuspectingly consenting to the collection and usage of their driving data. In our opinion, this, along with forcing customers to download GM's free mobile apps that only collected more data, constitute an example of the forced action deceptive pattern. Their use of extensive terms and conditions, which were worded in a confusing, vague manner, and made several remissions to other texts[284], appears to be an example of trick wording, and seems to have effectively deterred users from properly reviewing the terms – although, even if they did, they would never realize "GM's actual conduct", as it was never disclosed[285].

The confirmshaming pattern was also ever-present, for if the customer wanted to decline the connected vehicle services, they would be presented with warning messages

[279] Ibid, pp. 2-3
[280] Ibid, p. 3
[281] Ibid., p. 33
[282] Ibid.
[283] Ibid., p.14
[284] Ibid., 15. The users were presented with a 29-page long document called "user terms for connected vehicle services", an 18-page long privacy statement, a link to AT&T terms and conditions, as well as their network management practices and a vehicle ownership statement.
[285] Ibid., p. 16, 19-21

that stated, in bold, that customers would be deactivating several safety features from their vehicles[286]. If the client still declined, then GM would once again warn that safety features would be deactivated and utterly encouraged them to go back and accept the terms. But it did not end here – if the customer still declined, then GM would nag them, through email, to sign up for a trial-period of the connected vehicle services[287]. This pattern was also present when the customer did not download the aforementioned mobile apps – GM would send various emails reminding users to download and install them on their devices[288].

The hard to cancel pattern was also employed, for while the enrollment was simple enough, and could be done in many ways, in order to cancel, the customer had to call GM's services[289].

Even more interesting, the civil penalties imposed were aggravated "if the subject of the proceeding was calculated to acquire or deprive money or other property from a consumer who was 65 years of age or older when the act or practice occurred[290]", which clearly shows an additional preoccupation with a group that is considered vulnerable.

FTC v. Amazon.com and FTC v. Publishers Clearing House LLC[291] are another two very recent decisions issued by the District Court for the Western District of Washington and by the District Court for the Eastern District of New York, respectively, finally address these practices by its name and recognize their problematic nature.

In regards to the first case, the court recognizes the usage of deceptive patterns by Amazon in order to get customers to unknowingly enroll in their automatically renewing prime service (what is referred to as "nonconsensual enrollment/enrollees"), and also in their cancellation process, designed to be "labyrinthine[292]", confusing and arduous for consumers wishing to withdraw from their services. This process was only changed in April 2023, after pressure from the Commission.

---

[286] Ibid.
[287] Ibid., p. 17
[288] Ibid., p. 18
[289] Ibid., p. 17
[290] Ibid., p. 34
[291] FTC v. PCH LLC, Case No. 23-cv-4735, pp. 1-2 "Although Publishers Clearing House LLC ("PCH" or "the Company") is required to allow consumers to participate in its sweepstakes promotions without purchasing a product, PCH uses deceptive and manipulative statements and user interface designs (sometimes referred to as "dark patterns") to deceive consumers into believing that they must order products before they can enter a sweepstakes or that ordering products increases their odds of winning a sweepstakes."
[292] FTC v. Amazon.com, p. 3

In regards to the enrollment in the Prime service, it is noted that it can be done through multiple channels. However, it is the website that is the most concerning for it includes several examples of misleading language. The most prominent one is the fact that while Amazon states that they are giving a free trial for 14 days, and that afterwards, the price, there is no mention of the auto-renewable feature unless the costumer clicks on a small arrow right beside a large, yellow sign that reads "Get FREE two-day delivery with Prime" or scroll down after the small text beneath that reads "no thanks[293]".

Furthermore, Amazon also exploits some consumer's lack of knowledge[294] of the Prime and Prime Video services, the latter being less expensive. However, upon enrollment, Amazon fails to inform that users will be enrolled in the more expensive Prime rather than on Prime Video. Additionally, upon confirmation, they make it difficult for users to choose between both services, for the only options offered are "start your free-trial" or "change plan". Unless the consumer does this, Amazon will sign them up for the Prime service and, after confirmation, take them to the Prime Video storefront.

The court found several deceptive patterns being used by Amazon: forced action, interface interference (both visual and in the language used), obstruction, misdirection, sneaking and confirmshaming.

Following, Publishers Cleaning House LLC is a seller of discounted magazine subscriptions, founded in 1953 in Port Washington, that eventually expanded into merchandise offerings until it became its core business. So, this decision is particularly interesting for our investigation, as it has been highlighted by the Court that PHC specifically "targets older and lower-income consumers[295]", and, therefore, particularly vulnerable, as has been highlighted by LUGURI and STRAHILEVITZ in their study[296]. The main problem is that while PHC's official rules all state that all entries are eligible to win without needing to purchase anything, the company still bombards costumers with emails and takes them through an infinite loop of e-commerce pages, claiming that one final step is amiss. Not only that, but the links rarely take consumers to the final step, instead redirecting them to the e-commerce page. The court found that the company had violated

[293] FTC v. Amazon, pp. 32-34
[294] Once again, this shows the conclusions of LUGURI and STRAHILEVITZ, in regards to how deceptive patterns are more effective against vulnerable users. See, Luguri, J.B. and Strahilevitz, L. (2021), op. cit., pp. 47,70-71, 80-81,
[295] FTC v. PCH LLC, p. 2 and p. 7
[296] LUGURI, J.B. and STRAHILEVITZ, L. (2021), op. cit., p. 99

Section 5(a) of the FTC Act, in specific, the prohibition of employing unfair or deceptive practices in or affecting commerce.

The company has been found to use several deceptive patterns to lure their users into buying additional products in order to enter their sweepstakes — for example, sneaking, trick wording, visual interference, hidden costs, fake urgency, and nagging[297].

We also consider that there is some emotional manipulation involved, as the call-to-action button "WIN IT" or "Win for Life" are susceptible to creating a response in users, along with the usage, on the following pages, of arrows and symbols that represent that the user must, in fact, purchase something in order to win. As it was shown in the decision, the tactics become even more manipulative when the users did not complete any purchase, stating on the one hand that the costumer has made the right decision in continuing to follow the links, and on the other, that they should place an order ("we've packed this notice with amazing deals and free offers we hope you'll love. Won't you take a look and place your first order today?" and "Please don't say NO" on another page filled with product advertisement[298]). At the same time, they use small, low contrast text on the bottom of the page, where it is rarely seen, below the continue button, to state that "no purchase or fee necessary to enter. A purchase won't increase an individual's chance of winning".

Another example of the emotional triggering pattern we believe is present is the usage of official IRS language[299] to trick users into opening the company's emails, thus creating a sense of anxiety as some can be misled into thinking they have a tax obligation to fulfil. This is exacerbated by the fact that this is not the first time that PCH is sued for the employing of these tactics.

Lastly, the court decided that the company's harmful conduct towards customers would harm public interest in the absence of an injuctive relief — which further cements the idea that the usage of deceptive patterns is, indeed, harmful and needs to be urgently addressed[300].

In the US, most protection against the usage of deceptive patterns has its foundation consumer law provisions, and states seem to fight against them under this broad umbrella. The fact that both courts and the legislators have started to recognize the

[297] Ibid, p. 3
[298] Ibid, p. 28
[299] Ibid, p. 35
[300] Ibid, p. 52

existence and harmful consequences of deceptive patterns, and enforcing measures to ensure consent is obtained through transparent and non-deceptive methods hints towards a step in the right direction, especially in the data protection field, where consent is no longer considered valid if obtained using deceptive design patterns.

EU Law

When it comes to communitarian legislation concerning deceptive design patterns, we must highlight the GDPR[301] and, more recently, the DSA[302], which has prohibited, specifically, the use of these patterns in such a way that they distort users' free choice, on the aforementioned recital 67, and to the Digital Markets Acts (hereinafter, DMA). We also must look at the UCPD[303], and, lastly, we will also look at the AI Act and Data Act, as they both contain provisions to regulate this issue. Additionally, the Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 as regards financial services contracts concluded at a distance also needs to be mentioned, for it seems to include the description of practices that clearly constitute deceptive design patterns.

It is worth noting that, similarly to what happens in the US, most of the legislation prohibiting the use of deceptive conducts pertains to consumer law and that when it comes to the regulation of deceptive patterns, it somewhat falls in the middle of consumer protection and data protection, as the DSA, along with the proposed AI Act and Data Act highlight. It is worth reminding the reader that data protection law, and the way it can regulate deceptive patterns, is the focus of our project and, therefore, we will mainly focus on legal instruments pertaining that legal field.

[301] 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).
[302] 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)
[303] 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)

The Unfair Commercial Practices Directive

We will not be repeating what we said in regards the UCPD on the previous chapter, when it comes to our discussion on the average versus the vulnerable consumer other than that "the only protection for vulnerable consumers is to adapt the consumer cognitive benchmark to the characteristics of the vulnerable group that the commercial practice might foreseeably impact[304]". First, it is important to note that the UCPD has a list of practices that are blacklisted, which means that their practice will always be considered unfair and abusive. Secondly, this directive provides a safety net in Article 5 (2, b) of the UCPD, according to which a commercial practice is unfair if it materially distorts or is likely to distort the economic behavior with regard to 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 people, which ensures that any unfair practices that might not be listed anywhere else do not go without a penalty[305]. The notion of material distortion to the economic behavior of the consumer is present in Article 2(e) of the UCPD, which defines it as a commercial practice that impairs the consumer's ability to make an informed decision, causing them to take a transactional decision they otherwise would not, which is fairly similar to the concept of deceptive patterns we adopted. Interestingly, the aforementioned guidelines state that if a consumer might have to spend more time engaged in a process, this can constitute an unfair commercial practice[306], which seems to nod at the longer than necessary or hard to cancel patterns. It is always interesting to note that article 5 consecrates the notion of professional diligence, which can be reconducted to honest market practices and good faith, as interpreted in the aforementioned guidance document[307]. Codes of conduct for a specific field are also noted as being important instruments in establishing what are these honest practices[308].

[304] Malgieri, G. (2023), op. cit., p. 67
[305] 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, p. 36. Available for consultation on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)
[306] 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, p. 32.
[307] 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, paragraph 46.
[308] Ibid.

Additionally, pursuant to articles 6 and 7 of the same directive, any act that constitute a misleading practice that is likely to distort the transactional decision of the average consumer is prohibited. It is clear by the wording of Article 6 that the way the information is presented to the consumer can impact their decision which is why it is stated that a commercial practice might be misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the consumer, even if the information is factually correct. Examples of deceptive patterns included in Article 6 can be fake scarcity, fake social proof and fake urgency, as the way they are presented to the consumer trigger their scarcity and social proof bias, thus effectively misleading them when most of the times, there is no limited time to complete an action, and the testimonials are fake, as we saw above.

Moreover, Article 7 of the UCPD also regards as misleading practices those which, considering all circumstances (including the communication medium), omits material information that the average consumer needs to make an informed decision. It is also considered an omission, under these grounds, the company hides this information or provides it in an unclear, unintelligible, ambiguous, or untimely manner, or even if the commercial intent of the commercial practice is not identified, pursuant to Article 7(2). Examples of deceptive patterns that allow for this to happen are visual interference, preselection, hidden costs and subscriptions, disguised ads and comparison prevention, for they effectively confuse the consumer and either make it more difficult for them from finding the information on the platform or prevent them from doing so altogether. As LEISER and YANG argue, Article 7(2) and 7(3) of the UCPD, for "when deciding whether the trader omitted information, the regulator considers the limitations of space or time imposed by the communication medium and whether the trader thought about measures to make the information available to consumers by other means[309]".

It is also relevant, for the purpose of our investigation to mention that Article 8 of the UCPD considers as an aggressive commercial practice those that, in their factual context, use harassment, coercion and undue influence to impair freedom of choice or conduct. Article 9, in determining how to evaluate the use of harassment, coercion or undue influence, states that it is relevant to analyze not only the timing, location, nature or persistence of the tactic, but also the use of threatening or abusive language, if the

[309] LEISER, M., & YANG, W. (2022, November 12). Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive. https://doi.org/10.31235/osf.io/7dwuq, p. 21.

company is exploiting a circumstance of the consumer of such gravity that impairs their judgement to influence their decision (thus abusing their vulnerability, as we explored on the previous chapter), the imposition of disproportionate non-contractual barriers to exercise rights and the threat to take any legal action where it is not possible, legally, which are practices that can be achieved through patterns such as nagging, hard to cancel, confirmshaming, trick wording, sneaking, and obstruction, for these tend to coerce users into doing an action they would not, if their time and attention was not depleted, if they noticed and understood properly the implications of their action, or if the platform did not force them to.

Although the UCPD does not directly address deceptive patterns, it is undeniable that some of these practices constitute examples of such, as we had the opportunity to see, previously. Moreover, it is possible to establish a parallel between this directive and the FTC Act, even if we consider the UCPD more complete in scope.

The Digital Services Act

The DSA aims to contribute to the proper functioning of the internal market for intermediary services by setting out rules for a safe, predictable, and trusted online environment that facilitates innovation while effectively protecting the consumers. As stated before, the DSA contains in its recital 67 the definition of dark patterns we have adopted for the purposes of this dissertation and establishes the direct prohibition for providers of online platforms to deceive or nudge the recipients of the service and to distort or impair the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof.

Such practices include, but are not limited to, employing exploitative design choices to direct the recipient to actions that benefit the provider of online platforms at the expense of the user. Presenting choices in a non-neutral manner, such as giving more prominence to certain choices through visual, auditory, or other components, when asking the recipient of the service for a decision is also prohibited, along with repeatedly requesting the user to make a choice where such a choice has already been made, making the procedure of cancelling a service significantly more burdensome than signing up to it, or making certain choices more difficult or time-consuming than others, making it unreasonably difficult to discontinue purchases or to sign out from a given online platform allowing consumers to conclude distance contracts with traders, and deceiving the

recipients of the service by nudging them into decisions on transactions, or by default settings that are very difficult to change, and so unreasonably bias the decision making of the recipient of the service, in a way that distorts and impairs their autonomy, decision-making and choice. The same recital also states that these rules should be interpreted as covering prohibited practices falling within its scope to the extent that those practices are not already covered under the UCPD or the GDPR.

Furthermore, the DSA recognizes that the use of personalized advertisements based on users' interests and vulnerabilities can have serious negative effects and amplify societal harms, such as presenting a contribution to disinformation campaigns and discrimination against some groups. Thus, it is established that providers of online platforms shall not present advertisements using special categories of personal data, as prescribed on Article 9(1) of the GDPR[310].

When assessing these practices, we must look at Article 25(1), which clearly states that platforms are forbidden from designing, organizing or operating their interfaces in ways that deceive or manipulate the users, or in a way that material distorts or impairs their ability to make free and informed decisions. The potential effectiveness of this provision is "limited by specific gaps and ambiguities[311]", however, as it seems to be too broad and abstract to properly regulate this issue and thus, might require clarification in the future[312]. Another issue that the DSA raises is the fact that it is not applicable to micro and small enterprises, or to intermediary services, and thus, these providers are excluded. Although we understand the *ratio* of such exclusion, it would be useful to also include smaller entities to avoid the risk of circumventing the important rules and obligations this Regulation enforces.

Still, it is interesting to see that the DSA recognizes, on Recital 83, that deceptive design originates risks to the public health, minors and to a person's physical and mental well-being, or gender-based violence. As stated on the Recital, this category of risks emerges from concerns relating to the design, functioning or use, including through manipulation of VLOP's and or Very Large Online Search Engines (hereinafter, VLOSE's). Therefore, to assess and mitigate these risks, Recitals 84 and 87 clearly state that these platforms need to focus on the systems and elements contributing to the risks,

[310] Digital Services Act, Recital 69.
[311] LEISER, M. (2024). Psychological Patterns and Article 5 of the AI Act: Deleted Journal, 1(1), 5–23. https://doi.org/10.21552/aire/2024/1/4, p. 9.
[312] Ibid.

and that they should adapt any necessary design, feature or functioning of their service, such as the interface design, among others. These Recitals are consecrated on Articles 34 and 35, which state that, to assess the risk, providers of VLOP'S and VLOES's shall diligently identify, analyze and assess any of the risks originating from the design of their service, which shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, taking into account factors such as the any actual or foreseeable negative effects for the exercise of fundamental rights, including the right to protection of personal data or to the protection of public health and minors, as well as serious negative consequences to the person's physical and mental well-being. As SANTOS & LEISER argue, some measures can include the clear disclosure of material information, the prohibition of misleading or coercive tactics that influence user behavior, the assurance that the user has effective control over their data and preferences, and also, making sure that services are audited, to make sure they comply with privacy and consumer protection legal frameworks[313].

In conclusion, the DSA contain a rather broad scope of actions that constitute examples of deceptive patterns such as pre-selection, nagging, hard to cancel, forced action, obstruction, and trick wording. Although a remarking step in the right direction towards regulation, we are of the opinion that it still falls short in properly regulating the issue of deceptive design patterns.

The Digital Markets Act

Similarly, the Digital Markets Act[314] has also consecrated prohibitions regarding the use of deceptive patterns, noting that gatekeepers have a significant impact on the internal market and the recognition of how harmful unfair practices are to its functioning. Given the fact that gatekeepers collect a plethora of personal data of end users for various purposes (such as third-party personalized advertisement, custom audiences, and processing), this can signify that they have a potential advantage in terms of accumulation of data. Pursuant to the same Recital 36, similar advantages result from the conduct of

[313] SANTOS, C. & LEISER, M. (2024), op. Cit., p. 24.
[314] 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) (Text with EEA relevance), Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

combining end user personal data collected from a core platform service with data collected from other services, cross-using personal data from a core platform service in other services provided separately by the gatekeeper, notably services which are not provided together with, or in support of, the relevant core platform service, and vice versa or signing-in end users to different services of gatekeepers in order to combine personal data. To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalized but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent.

In addition to this, Recital 37 clearly states that this alternative cannot be of different or degraded quality compared to the service provided to the user who provided consent, and emphasizes that gatekeepers shall make sure to present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner, which shall be given on the terms of the GDPR (therefore, freely given, specific, informed and unambiguous). It is also established that gatekeepers shall not design, operate and organize their interfaces in a way that deceives, manipulates or otherwise distorts or impairs the ability of the user to freely give consent. It establishes a limit to the "nagging" pattern, for gatekeepers shall not prompt users more than once a year to give consent for the same processing purpose they initially did not agree to.

Pursuant to Recital 41, gatekeepers also cannot interfere with a user's decision to acquire content, subscriptions, features or other items outside the core platform services of the gatekeeper, nor can they impede users from uninstalling any pre-installed applications or software, unless they are essential for the functioning of the operating system or device, as stated in Recital 49.

It is also interesting that Recital 63 seems to directly prohibit gatekeepers from using obstructive patterns, as it states that, since gatekeepers shall not be allowed to make it unnecessarily difficult or complicated for business users or end users to unsubscribe from a core platform service. Closing an account or un-subscribing should not be made be more complicated than opening an account or subscribing to the same service. Gatekeepers should not demand additional fees when terminating contracts with their end users or business users. Gatekeepers should ensure that the conditions for terminating contracts are always proportionate and can be exercised without undue difficulty by end

users, such as, for example, in relation to the reasons for termination, the notice period, or the form of such termination.

Article 13(6) is, therefore, aimed at prohibiting gatekeepers from using deceptive design patterns. Pursuant to this article, the gatekeeper shall not degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices laid down in Articles 5, 6 and 7, or make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof. Article 5, in turn, establishes that gatekeepers cannot accumulate and cross-use personal data without user's consent which, as we explained above, needs to be given in the terms established on the GDPR.

The AI Act

The AI Act[315] aims to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation. It is worth noting that Article 5 of this Regulation lays down several prohibitions of AI practices, such as placing on the market or using AI systems which use subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behavior of a person or group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to make a decision they otherwise would not and causes, or is likely to cause, significant harm to that person or to a group of persons. It is also forbidden, pursuant to item (b), to place on the market or use AI systems that exploit any of the vulnerabilities of a natural person or group of persons due to their age, disability, or specific social or economic situation, with the same objective described previously. It is interesting to note that we can extract four criteria to assess whether or not a system could fall under the Regulation's provisions, as LEISER highlights: the AI Act is applicable to systems that manipulate

[315] Regulation (EU) 2024/168 of the European Parliament and of the Council of 13 June 2024.

behavior beyond the conscience of the individual (nature of the system), through the use of subliminal techniques that exploit a user's awareness (method of manipulation), which might cause significant harm to the user or others (potential for harm) and that might specifically target vulnerable individuals or groups (target of manipulation)[316]. As the same author highlights, the prohibitions set forth in Article 5 (a) and (b) are vague, especially when it concerns the term beyond consciousness, which makes it difficult to assess, posteriorly, the moment when manipulation stops being conscious and starts being unconscious[317]. On this point, and with all due respect, we tend to partially disagree, for we are of the opinion that manipulation is always unconscious, especially when deceptive design patterns are used. As we had the chance to examine on the first chapter, they exploit our cognitive biases and bounds, which we, as human, are not aware of. Still, we agree with LEISER on regards of the vagueness of the expression. This author also notes, rightfully so, that it might be complicated to establish a link of causality between the subliminal tactic and the suffered harm[318].

Lastly, we can look at the previously mentioned Directive (EU) 2023/2673[319] which complements the DSA. As stated in Recital 41, while the DSA prohibits intermediary service providers operating online platforms from using dark patterns in the design and organization of their online interfaces, this Directive should oblige Member States to prevent traders offering financial services at a distance from using such patterns when concluding contracts for such services. Accordingly, Article 16e describes several practices that constitute deceptive design patterns, such as giving more prominence to certain choices when asking the consumers who are recipients of their service for a decision, repeatedly requesting that consumers who are recipients of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience and making the termination of a service more difficult than subscribing to it.

[316] LEISER, M. (2024). Op. Cit., p. 10
[317] Ibid., p. 17.
[318] Ibid.
[319] Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC (Text with EEA relevance), available on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202302673

Battling deceptive patterns in privacy: GDPR and the Data Act

There are several key obligations arising from the GDPR concerning the design of user-interfaces and content presentation of web services and applications. As highlighted by the Guidelines 03/2022[320] "these principles must be implemented in a substantial way, and, from a technical perspective, they constitute requirements for the design of software and services".

The GDPR regulates the protection of personal data and the free movement of such data. It establishes that the data subject's personal data must be processed by the controller lawfully, fairly and transparently (principles of lawfulness, fairness and transparency)[321].

While the principles of lawfulness and transparency are directly mentioned in the GDPR, with the first one meaning that the processing of personal data must stand on legal grounds, and the second concerning the fact that information must be presented in a concise manner, be easily accessible and easy to understand[322], the principle of fairness although considered to be a "critical tennet of data protection law"[323] [324] and essential where it concerns battling deceptive patterns, in our opinion, it is not fully explained in the GDPR[325]. The EDPB does define the principle of fairness as "an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject[326]", putting in evidence the idea that a fair treatment is one that does not allow for power imbalance between the controller and the data subject to thrive. In the cited Guidelines, the EDPB also states that "data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or

[320] Guidelines 03/2022, ibid.
[321] Article 5, number 1 (a) GDPR
[322] Recital 58 GDPR, which includes the obligation of using plain language and visualization where appropriate, specifically in situations where the number of actors and technological complexity of practice make it difficult for the data subject to be aware of the processing of their data, such as online advertising.
[323] HÄUSELMANN, A., & CUSTERS, B. (2024). Substantive fairness in the GDPR: Fairness Elements for Article 5.1a GDPR. Computer Law & Security Review, 52, 105942. https://doi.org/10.1016/j.clsr.2024.105942, pp. 2-3
[324] The EU Charter of Fundamental Rights (hereinafter, The Charter) mentions the principle of fairness in Article 8 (2), which states that personal data must be processed fairly, for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
[325] KUNER, C., BYGRAVE, L. A., DOCKSEY, C., DRECHSLER, L., & TOSONI, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected articles. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3839645, p. 68.
[326] EDPB Guidelines 4/2019, on Article 25 (Data Protection by Design and by Default), (20.10.2020), p. 17. Available here: edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (europa.eu)

design[327]", which further confirms our opinion that the usage of deceptive design patterns substantially violates this principle, which is aggravated when before a vulnerable individual.

Fairness can be procedural or substantive, and whereas the former regards the fairness of the procedure by which data was collected and processed, the latter concerns the effects that the processing has on the data subjects[328]. Both dimensions are essential for the scope of our dissertation, as this principle is crucial in preventing the power imbalance existent between the controllers and the data subjects, which happens during the collection of data and reflects itself on the impact it might have on the individual. Thus, we must consider not only the expectations and the effects on the data subjects, but also the interests of the parties, to prevent the exploitation of individual vulnerabilities, which is inherently unfair[329]. We wholeheartedly agree with MALGIERI, concluding that "at least one way to articulate fairness might be the protection of individual vulnerabilities and the prevention of vulnerability exploitation, as consequences of significant power imbalance between individuals[330]".

The data subject's personal data also must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those (principle of purpose limitation)[331] and treated in a an adequate, relevant and limited in relation to the purposes for which it is processed (principle of data minimization)[332], the controller being responsible for the compliance with these (and the other) principles established.

The processing of personal data must be grounded on a legal basis (lawfully), as prescribed by article 6 GPDR, which states that the processing shall only be lawful if that basis is fulfilled. For the purposes of our dissertation (and given the space limitation we have), we will only be focusing on the first one, consent for the processing of personal data[333], which must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the

[327] Ibid., p. 18
[328] HÄUSELMANN, A., & CUSTERS, B. (2024), Op. Cit., p. 4
[329] MALGIERI, G. (2020). The Concept of fairness in the GDPR: A Linguistic and Contextual interpretation. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3517264_code2392402.pdf?abstractid=3517264&mirid=1, p.10
[330] Ibid.
[331] Article 5, number 1 (b) GDPR
[332] Article 5, number 1, (c) GDPR
[333] Article 6, number 1, (a) GDPR

processing of their personal data, as stated in Recital 32, regarding the conditions for consent. This Recital also establishes three very important notions: the first is that silence, inactivity or pre-selected boxes shall not constitute consent, the second is that if the processing has multiple purposes, all of them must be consented to individually and lastly, the third is that the request for user consent shall be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. The conditions for consent are expressed on Article 7, which has a couple interesting aspects. First and foremost, we can highlight that it is the controller's responsibility to demonstrate the consent of the data subject to the processing of their personal data, pursuant to the article 7 (1) GDPR, and that they did not abuse their autonomy and ability to make free and informed decisions through the use of deceptive patterns. Secondly, pursuant to number 2 of this article, the request for consent needs to be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using plain and clear language, or else, the consent obtain will be non-binding. Additionally, number 3 also states that not only the data subject shall be able to withdraw their consent at any time, but also, that it must be as easy as giving consent and, lastly, if the provision of a service or performance of a contract are conditional on consent that can potentially mean that the consent was not freely given by the data subject.

From here we can already pinpoint that, although the GDPR does not specifically mention deceptive patterns, it is clear that consent obtained through the use of, for example, preselection, obstruction, trick wording and visual interference is not valid, with Recital 32 of the GDPR explicitly forbidding the usage of pre-selected boxes to obtain consent. Additionally, Recital 42 prescribes that consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance, which also hints at the blatant prohibition of obtaining consent through the use of the forced action pattern.

In regards to the rights of the data subject to information, Article 12 prescribes that the information to be provided to the user regarding the processing of their data needs to be given in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, especially when this information is presented to children. We are of

the opinion that this provision can be read so as to include other kinds of vulnerable individuals, not only children.

We are also of the opinion that the usage of deceptive patterns to obtain consent violate the principles of data minimization and purpose limitation[334], too, for, obviously, they are designed to gather more data than what is necessary. Pursuant to the cited items of article 5, data must be collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes (purpose limitation) and must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, which does not happen in the aforementioned cases.

Lastly, the principle of data protection by design and default is also put at stake by deceptive patterns, for the default, when an interface or platform employs these patterns, is not a privacy-friendly option. This goes blatantly against Article 25, which establishes that controllers must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. Additionally, these measures shall also be implemented to ensure that, by default, only personal data needed for each specific purpose is processed.

When it comes to vulnerability, it is interesting that Article 9(1) establishes that the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation and health is prohibited, for this kind of data is sensible and might make a person more vulnerable, in our opinion.

It is extremely important to look at Article 82 of the GDPR, which establishes the right to compensation to "any person who has suffered material or non-material damage as a result of a GDPR infringement". As defined in Recital 75, there can be physical, material, and non-material damages, such as financial losses, in the second case, or personal disadvantages, like discrimination or reputational damage, as noted in Recital 85.

There are three cumulative conditions that must be met in order for the right to compensation to emerge: the organization has to infringe the GDPR, a damage must result

[334] Article 5, 1 (b) and (c) GDPR

for the data subject and there must be a causal link between the infringement and the suffered damages[335]. The burden of proof rests on the data subject, but the controller also needs to demonstrate that they did not cause the harm, as explained in Article 82(3).

We are of the opinion that the usage of deceptive design patterns, where they put a data subject's rights at stake, could theoretically constitute damage susceptible to compensation, but as SANTOS et al. note, it would be difficult to prove both the damage requirement, as most studies thus concern user's perception of harm rather than actual harms suffered, and the infringement one, as, although this is slowly changing, neither the EDPB or the jurisprudence have specifically decided on what patterns violate the GDPR[336]. This is without prejudice that we still consider that deceptive patterns are, by nature, inherently violating of the principles of fairness, lawfulness, and transparency, in general, and thus, both national authorities and the courts need to start seriously considering them and the impact they have on data subjects.

When we coordinate the UCPD with the GDPR, we can conclude that even if a company violates the GDPR or the ePrivacy Directive, that does not always equate to a violation of the UCPD. However, when the violations of data protection pertain the transparency of the commercial practices, Article 7 (2) and number 22 from Annex I of the UCPD clearly prohibit companies to hide the commercial intent behind the practice, for example, data collection and processing for commercial purposes[337]. As mentioned on the cited guidelines, "personal data, consumer preferences and other user-generated content have economic value and are often being made available to third parties[338]" and thus, to not inform the user of such use, might constitute a misleading omission of material information, as well as a violation of transparency and the information requirements under the GDPR.

When it comes to the Data Act[339], we can start by mentioning the fact that dark patterns are also mentioned on Recital 38 of this Regulation, regarding the data

[335] SANTOS, et al. (2024), op. cit., p. 22
[336] Ibid., p. 24
[337] 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, p. 19. Available for consultation on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)
[338] Ibid.
[339] 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) (Text with EEA relevance), available for consultation here: https://eur-lex.europa.eu/eli/reg/2023/2854

minimization principle. The content of this recital is reflected in Article 4(4) of the Regulation, pursuant to which data holders shall not make the exercise of choices or rights by the user unduly difficult, including by offering choices to the user in a non-neutral manner or by subverting or impairing the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user digital interface or a part thereof.

Moreover, Article 11 prescribes that a data holder may apply appropriate technical protection measures to prevent unauthorized access to data, including metadata and that such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use, or access data. Numbers 2 and 3 of the same article establish that if the data is obtained through the deployment of deceptive or coercive means (number 3, item a), there is an obligation of erasing the data made available to the data holder and any copies thereof, informing the user of the unauthorized use or disclosure of the data and the measures taken to put an end to it and, also, of providing compensation to the party suffering from the misuse or disclosure of the unlawfully accessed data.

Case Law

As it has been highlighted by the 2022 behavioral report commissioned by the European Commission, before the high dissemination of deceptive patterns across all platforms of all dimensions (not only the Very Large Online Platforms — hereinafter, VLOP's), it is necessary to analyze whether or not the current legislation is enough to face the challenges these tactics pose[340].

It is relevant, thus, to analyze the CJEU's decisions, as well as European Data Protection Authorities (hereinafter, DPA), in this matter in order to properly understand the stance of the European Union, which has started to gradually address deceptive design patterns by name[341].

[340] European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F. (2022). Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation : final report, Publications Office of the European Union, p. 6, https://data.europa.eu/doi/10.2838/859030

[341] SANTOS, C., ROSSI, A., *The emergence of dark patterns as a legal concept in case law.* (31 July 2023). Internet Policy Review. https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept.

In February 2023, the Italian DPA issued the first decision where the term 'dark patterns' was expressly mentioned[342], having found that Ediscom S.P.A was making use of several of these tactics such as forced action (as the user had to answer to several questions regarding not only their personal data, but also some relating to their purchasing capacity and habits and annual income, for example), visual interference (for the user was shown several pop-ups, especially after rejecting consenting for the processing of their data for marketing purposes), and also, as SANTOS and ROSSI note, the fact that Ediscom also required users to enter contact information of their relatives, can also configure a deceptive pattern (social pyramid[343]).

Other DPA's have been following suit and increasingly scrutinizing the usage of deceptive patterns, such as CNIL (France), who issued a 150 million euro fine against Google, who had been nudging users to accept cookies by making them navigate several steps to refuse them, whereas a single click was needed to accept them[344]. The Norwegian DPA, Datatilsynet, also ordered an injuction against Grindr for sharing user-data with third-parties with consent obtained through the use of deceptive patterns (therefore, invalid), for not only were the users never informed that their data would be shared with third-parties, but also, this regards sensitive data and these users could be potentially deemed vulnerable given their sexual orientation[345].

Furthermore, it is possible to pinpoint that the European Commission has opened formal proceedings to investigate whether X has employed the social proof pattern in their interface in regards the blue-check, as noted by SANTOS and LEISER[346].

We can also emphasize EDPB's Binding Decision 2/2023[347] on the dispute submitted by the Irish SA regarding TikTok Technology Limited, who infringed the principle of fairness on the processing of children's personal data, by utilizing deceptive design practices in the platform, for it was considered that children registering in the platform were not adequately informed of the implications of doing so, as all accounts

[342] Italian Data Protection Authority's decision issued against Ediscom Sp.A, (February, 2023), in which the authority decided that the company used dark patterns to circumvent the will of the person concerned. https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014
[343] SANTOS, C., ROSSI, A. (2023), Op. Cit.
[344] CNIL vs. Google LLC and Google Ireland Limited, (13.07.2023). https://www.cnil.fr/en/closure-injunction-issued-against-google
[345] Datatilsynet vs. Grindr LLC (13.12.2021), https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/record-fine-grindr-confirmed/
[346] SANTOS, C., & LEISER, M. (2024). Op. cit., p. 23.
[347] Binding Decision 2/2023 (02.08.2023) on the dispute submitted by the Irish SA regarding TikTok Technology Limited, edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf (europa.eu)

were set to being public-by-default and the option to make the accounts private was not set in a neutral, objective way.

When it comes to court decisions, we can highlight Case C-673/17[348], regarding the consent of participants in a promotional lottery organized by a company to the transfer of their personal data to the company's sponsors and partners, to the storage of information and to the access of information and equipment. To participate, users had to tick a checkbox consenting to the receiving of third-party advertisements, and during the registration, there was a pre-selected box users had to opt-out of if they did not want their online behavior tracked. Although the CJUE does not refer to pre-selected boxes as deceptive patterns, it did decide that consent had to be freely given, and in accordance to Article 4(11) GDPR, which, in this instance, it was not.

Another decision that we looked at was Case C-61/19[349], which pertains to the same practice of using pre-selected boxes as a way of gathering user consent. The CJEU upheld that consent was not valid if the box was pre-selected, if the terms of the contract were misleading the data subject whether they could reject consent and still conclude the contract and, finally, if additional steps were required to withdraw or refuse consent, which are all practices that can be subsumed into the deceptive patterns categories of pre-selection and hard to cancel.

Deceptive design patterns are a way of presenting content in a way that substantially violates GDPR's requirements, while formally pretending to be compliant[350]. As explained previously, the use of techniques that take advantage of our attention and cognitive biases can have a direct impact on user's ability to uphold their rights[351]. This is exacerbated when the individual in question lacks the ability to properly understand or give their free, informed, specific, and unambiguous consent to the processing of data — which, as we concluded above, translates into a formal and substantial unfairness, given the power imbalance between controller and data subject - and an individual in this position shall be deemed vulnerable. We absolutely cannot forget that, at the end of the day, what is at stake is nothing more nothing less than the protection of a fundamental right: the right to privacy.

[348] Case-673/17 (01.10.2019), *Planet49 v. Federation of Consumer Organizations, Germany.* Available for consultation on: https://curia.europa.eu/juris/document/document.jsf?docid=218462&doclang=EN
[349] Case 61/19 (11.11.2020), Orange România SA V. Romanian Data Protection Authority. Available for Consultation on: https://curia.europa.eu
[350] Guidelines 03/2022, p. 8
[351] CHATELLIER, R., DELCROIX, G. HARY, E., et al., *op. cit.,* (2019) p. 10

GOING FORWARD – REFLECTIONS FOR THE FUTURE

Up until this point in our dissertation, we presented the problematic of deceptive design patterns and how they impact vulnerable data subjects' autonomy and decision making. Therefore, after examining the concept of vulnerability and the legal framework surrounding these harmful practices, we believe it is important to look at the future. It is the time to ask: what can we do to put a stop, or at least to slow down, the proliferation of deceptive design?

We humbly propose a multidimensional approach to tackle this issue, anchored in three different pillars: regulation, cooperation, and education.

The pillar of regulation, as we had the opportunity to present, is already being built, and thus, we will refrain from repeating in this section what we have already said in these regards. The setting stones were put in place and, more and more, deceptive design patterns are gaining the legal traction that is necessary to mitigate them and their impact, as it has been highlighted by several scholars and experts, such as BRIGNULL[352], SANTOS and LEISER[353].

It is, thus, necessary to promote not only the revision of existing laws, such as the GDPR and the UCPD, in order to properly battle the existence of these manipulative practices, but also the creation of specific provisions to penalize the platforms who use them. It is also urgent to accommodate the existing legislation in order to include vulnerable users, and to better protect them. We agree with MALGIERI[354], who argues that the Data Protection Impact Assessment (hereinafter, DPIA), consecrated in Article 35 of the GDPR, is a valuable tool to aid in the mitigation of vulnerabilities, as we can evaluate the kind of vulnerability and propose mitigation measures, but still, this might not be enough to correct the existent imbalance between data controller and vulnerable data subject. We are also of the opinion that harsher penalizations may be necessary, especially when the infractions regard vulnerable users.

The second pillar we propose is cooperation between stakeholders – designers and online platforms, as well as regulators, need to work together in order to put in practice the codes of ethics for design that already exist, as noted by BRIGNULL[355]. There needs to

[352] BRIGNULL, H. (2023), op. cit., p. 222.
[353] SANTOS, C. and LEISER, M. (2024), op. Cit., p. 30.
[354] MALGIERI, G. (2023), op. cit., p. 179.
[355] BRIGNULL, H. (2023), op. cit. p. 179-180.

be a standard for ethical design, in our opinion, which must uphold the principles of transparency, fairness and respect for user autonomy. It is not just a matter of following the law, it is a matter of "commitment to moral integrity and a recognition of the broader societal impact of design choices[356]". It is a matter of making platforms safer, more trustworthy, and more inclusive to all – but especially, to those who can be vulnerable.

BRIGNULL also notes that, potentially, we could user bright, or fair, patterns to battle deceptive design, but we are of the same opinion as this author and consider them useful, for they could standardize design practices, but that would be at the cost of innovation and improvement[357]. We believe, though, that designers can – and should – frequently test their designs to ensure that they are fair and do not deceive users. It is possible to do this by using a cognitive walkthrough[358] (a "technique user to evalute the learnability of a system from the perspective of a new user[359]") and place themselves in the position of the user by seeing if there is a possibility that the users are providing more data than necessary, consenting as a condition for the provision of a service, if they are misinterpreting the choices, or their availability, if certain key elements are obscured or in an unexpected location, if there are unnecessary steps impeding users from making their autonomous choice, if they are rushed into making a decision, or if they are manipulated into choosing a less privacy-friendly option and if they feel any negative emotions (guilt or anxiety) when declining a choice, for example[360].

The EDPB Guidelines 03/2022, applicable to social media platforms, also establish some useful recommendations for designing user interfaces fairly and in a way that not only effectively respect and implement the GDPR, but also serve as empowerment tools to the user, such as using shortcuts (like links that redirect the user to the most important aspects of privacy policies, for example, so that users can freely change their settings whenever they wish to and effectively manage their personal data), bulking options that have the same purpose, clearly stating the company's contact information and including a direct way (and identification) of the competent DPA, include a collapsible table of contents on the privacy policies to help users identify more

[356] ESTEFANI, J. N. A. (2024, February 22). Designing With Integrity: The Ethical Designer's Handbook On Dark Patterns - Raw.Studio. Raw.Studio. https://raw.studio/blog/designing-with-integrity-the-ethical-designers-handbook-on-dark-patterns/
[357] BRIGNULL, H. (2023), op. cit. p. 181
[358] ROSALA, M. (2024, January 30). Deceptive patterns in UX: How to recognize and Avoid them. Nielsen Norman Group. https://www.nngroup.com/articles/deceptive-patterns/
[359] FLAHERTY, K. (2024, February 13). Evaluate Interface Learnability with Cognitive Walkthroughs. Nielsen Norman Group. https://www.nngroup.com/articles/cognitive-walkthroughs/
[360] ROSALA, M. (2024), ibid.

quickly the relevant options, highlighting changes to the privacy policy, using coherent wording across the website – and applications, if applicable - to avoid confusion, providing definitions and making sure that data protection elements are visually striking[361]. It is also advisable to "include data protection points within the onboarding experience[362]" to facilitate users' setting their preferences, to use examples to illustrate the purposes of data processing, explaining the consequences of their actions – such as activating or deactivating a data protection control, or giving consent - in a neutral way, implement self-explanatory URL's in pages related to data protection settings, and include a form to help users exercise their rights, to name a few examples of good practices recommended by the EDPB in avoiding these tactics[363].

Lastly, and unsurprisingly, our last pillar is education and public awareness. Even if subjects such as user-centered design, persuasion, and design ethics are already mandatory in higher education courses, that is not enough[364] and further actions are necessary. The public – especially when we are all, potentially, vulnerable data subjects – need to be made aware of these practices, the public needs to know that they are used, and they need to know how to resist them, whenever possible. Digital literacy courses could be an option, especially if tailored for more vulnerable individuals, along with imposing, as we have already argued, stricter disclosure requirements in regards to privacy notices. The World Wide Web Foundation, along with Superbloom design, for example, have developed an initiative called "strategies for change", which aims to steer the technological world away from using deceptive design and towards fairer practices[365].

Knowledge is power – and the more knowledge a user has about their rights and about what companies are doing to put them at stake, the fiercer they can become in fighting against them and the more empowered they are in their autonomy.

[361] EDPB Guidelines 02/2023, op. cit., pp. 73-74
[362] Ibid, p. 74
[363] Ibid.
[364] BRIGNULL, H. (2023), op. cit. p. 180.
[365] Together against deceptive design. (2023, June 6). Superbloom. https://superbloom.design/learning/blog/together-against-deceptive-design/

CONCLUSION

The present dissertation has critically explored the pervasive issue of deceptive design patterns, in particular, their impact on vulnerable data subjects under EU legislation. Deceptive design patterns – practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions – pose a significant threat to user autonomy, as we had the chance to analyze, for they substantially hinder their ability to give free, informed, rational consent to the processing of their personal data, while violating the broader framework of data protection, especially the principles of transparency, fairness, lawfulness and data protection by default and by design. By focusing on the manipulative tactics used within the digital environment, our research has sought to provide a comprehensive analysis of their psychological foundations, legal background and implications, and the consequent harm to individuals, especially those deemed vulnerable.

The first chapter focused on outlining the definition, evolution, and conceptualization of design as a tool for communication between two parties, which is in permanent evolution. For that effect, we adopted the ICD's explanation of design and defined it as a discipline of study and practice focused on the interaction between a user and the man-made environment, taking into account aesthetic, functional, contextual, cultural and societal considerations. We then described the ground principles of design and the psychology lying behind them, as well as the cognitive bounds and biases we, as humans, are all subject to, because deceptive design patterns are built through the misapplication and exploitation of these factors. This work has shown how these patterns, from subtle nudges to outright coercion, exploit cognitive biases such as the anchoring effect, choice overload, default bias, and framing bias. The analysis revealed that these manipulative strategies undermine the very foundations of informed consent and autonomy as enshrined in key legal texts, such as the GDPR, in the field of data protection.

The dissertation then explored the concept of vulnerability, and how it should have a nuanced application in data protection contexts, much like several authors have already proposed before. Vulnerability, as argued through the presented layered vulnerability theory, is not static but context-dependent, with varying degrees, influenced by a plethora of factors such as socio-economic status, cognitive capacity, age, and digital literacy, for example. Vulnerable users are at greater risk of harm from deceptive design patterns due

to a reduced capacity to recognize, understand and resist such serpentine tactics, which act as a vulnerability driver. This dynamic understanding of vulnerability accentuates the need for tailored regulatory responses that move beyond a one-size-fits-all approach to data protection.

It is central to this discussion to understand that deceptive design patterns operate in a grey area of user manipulation, often falling between unethical design and unlawful practice. As we had the opportunity to emphasize, the GDPR does set forth principles, such as transparency, lawfulness, fairness, data protection by design and by default and data minimization, but it still lacks explicit provisions targeting these specific manipulative tactics. This legal ambiguity has been allowing companies to exploit user behavior subtly and systematically, thus violating user autonomy without breaching specific provisions of current data protection laws.

Therefore, a significant contribution of this dissertation is the comparative analysis of the regulatory frameworks in the EU and in the US it provides the reader with. It is true that in the field of consumer law there is a little more space for maneuvering in regards the use of deceptive tactics against the consumer, but the same does not apply to the data protection field.

While the EU has historically led the way in comprehensive data protection through the GDPR, only recently it has started to acknowledge, in explicit terms, the harmful existence of deceptive design patterns. The recent DSA and DMA, as well as the AI Act and the Data Act, introduce promising steps by including the concept of "dark patterns" and by proposing specific obligations to combat them. Additionally, the Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 as regards financial services contracts concluded at a distance has, too, recognized some deceptive patterns and prohibited them, along with urging Member States to take more stringent provisions against them. Although we consider this to be very positive, we are of the opinion that the EU still needs to fully address the nuanced challenges these tactics pose, despite the recent case law, especially in the data protection field, for the efforts still remain quite fragmented and lack the enforceable clarity necessary to combat the widespread use of deceptive patterns effectively.

In contrast, the US, through the FTC and recent state-level legislation, has begun to directly address these manipulative tactics. The cases against General Motors, Amazon and Publishers Clearing House show a growing recognition of the harms caused by

deceptive patterns and are setting, in our opinion, an important precedent in demonstrating the feasibility of holding companies accountable for using practices that dent consumer autonomy. In comparison to the EU stance, the US tackles this issue through a more aggressive stance (namely through the Time is Money initiative and the DETOUR Act), and we believe that the EU legislators should, too, adopt a similar position to fill the existent legal gaps.

In our dissertation, we further argue that these regulatory efforts must also be reinforced by a more in-depth understanding of human psychology and behavioral economics. Deceptive design patterns are not solely about a legal loophole to be exploited, but fundamentally about abusing and taking advantage of predictable patterns of human cognition. Indeed, this becomes particularly problematic when applied to vulnerable subjects, whose ability to make autonomous and well-informed decisions can already be compromised by factors such as digital literacy, cognitive overload, or socio-economic pressures. As we stated above, currently, the existent legal framework does not sufficiently account for these dimensions, which are critical to ensure the validity of the given consent.

Furthermore, the harms caused by these patterns go beyond the privacy concerns. We argue that they represent a direct offense to the fundamental human rights of dignity and autonomy to lead their lives and choices. The inability to freely consent, intensified by the manipulation of cognitive bounds and biases, results in considerable economic, emotional, and psychological harms that disproportionately affect those who can be in a more vulnerable position. As noted, deceptive patterns can lead to a cascade of negative outcomes, including economic exploitation, discrimination, and digital exclusion.

To address these unrelenting issues, we argue, through this dissertation, for a multidimensional approach. The first step, which is already in progress as we examined, is for regulatory bodies to present an explicit definition and categorization of deceptive design patterns in legal terms, which would involve not only revising the GDPR and other existing laws, but also creating new frameworks that directly target manipulative digital practices and include specific provisions to penalize companies who utilize deceptive patterns, with aggravated penalties for those affecting vulnerable users. On the same line, we are also of the opinion that the concept of vulnerable data subject should be specifically consecrated on the GDPR.

The second step to achieve the multidimensional approach we mentioned is the establishment of greater cooperation between the relevant stakeholders (regulators,

designers and the online platforms), in order to put in practice the existent ethical standards for UI and UX design. As explained, these standards need to stress the importance of transparency, fairness, inclusion, and simplicity in these fields. Initiatives such as the EDPB guidelines 02/2023 are yet another step in the right direction, but we are still of the opinion that it is not enough, and they need to be expanded to allow for a broader spectrum of digital environments.

Unsurprisingly, the last step we propose is public awareness and education, which we consider to be the cornerstone in combating the usage of these patterns. In the digital age, where most of our lives is behind a screen, and when all of us are, potentially, vulnerable data subjects, digital literacy programs focused on helping users recognize and resist manipulative tactics are necessary. Enterprises and companies also need to be subject to more robust disclosure requirements regarding their privacy policies and notices.

To conclude, the rise of deceptive design patterns represents, more and more, a significant challenge in the field of data protection, in particular. As we attempted to demonstrate throughout this dissertation, these practices hinder the foundational principles of user autonomy, informed consent, fairness, and transparency, and can have particularly harmful effects on vulnerable data subjects. In order to tackle this issue, a joint effort between legislative reform, cross-sector collaboration and user empowerment is required, for only through such a comprehensive approach we can strive to create a digital ecosystem that is respectful of all individuals and adequately protects their rights thus ensuring that the benefits of digital innovation do not come at the expense of fundamental rights and freedoms. So, as a collective, we must be able to recognize, regulate, and ultimately eradicate deceptive design patterns from the digital landscape.

BIBLIOGRAPHIC REFERENCES

Doctrine

Norman, D.A. (2013) The Design of Everyday Things: Revised and Expanded Edition, Basic Books, ISBN 978-0-465-00394-5.

Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark patterns: past, present, and future. ACM Queue, 18(2), 67–92. https://doi.org/10.1145/3400899.3400901

Santos, C., Morozovaite, V. and De Conca, S., (June 26, 2024) No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. Available at SSRN: https://ssrn.com/abstract=4877439

Kalman, T. (1991), Good History, Bad History, *Design Review*, 1(1), pp. 44-57, as cited in Barnard, M. (2013), Graphic Design as communication. In Routledge eBooks. https://doi.org/10.4324/9781315015385

Rodgers, P. A., & Bremner, C. (2017). The concept of the design discipline. Dialectic, I(1). https://doi.org/10.3998/dialectic.14932326.0001.104

Latour, B. (2012). 9. A Cautious Prometheus? A Few Steps Toward a Philosophy of Design with Special Attention to Peter Sloterdijk. In Amsterdam University Press eBooks (pp. 151–164). https://doi.org/10.1515/9789048514502-009

Brignull, H. (2023) Deceptive patterns: Exposing the Tricks Tech Companies Use to Control You. Testimonium Limited

Rodgers, P., & Bremner, C. (2011). Alterplinarity: “Alternative Disciplinarity” in Future Art and Design Research Pursuits. Studies in Material Thinking, 6, 1–16.

Kobourov, S.G., Mchedlidze, T., Vonessen, L. (2015). Gestalt Principles in Graph Drawing. In: Di Giacomo, E., Lubiw, A. (eds) Graph Drawing and Network

Visualization. GD 2015. Lecture Notes in Computer Science(), vol 9411. Springer, Cham. https://doi.org/10.1007/978-3-319-27261-0_50

Wagemans, J., Elder, J. H., Kubovy, M., Palmer, S. E., Peterson, M. A., Singh, M., & Von Der Heydt, R. (2012). A century of Gestalt psychology in visual perception: I. Perceptual grouping and figure–ground organization. Psychological Bulletin, 138(6), 1172–1217. https://doi.org/10.1037/a0029333

Reyna, A. (2018). The psychology of privacy—what can Behavioural Economics contribute to competition in digital markets? International Data Privacy Law, 8(3), 240–252. https://doi.org/10.1093/idpl/ipy017

Becker, G. S. (1976). *The economic approach to human behavior*. https://doi.org/10.7208/chicago/9780226217062.001.0001

Jolls, C., Sunstein, C. R., & Thaler, R. H. (July 1998), *A behavioral approach to law and economics*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=74927

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, *69*(1), 99. https://doi.org/10.2307/1884852

Korteling, J. E., Paradies, G. L., & Meer, J. P. S. (2023). Cognitive bias and how to improve sustainable decision making. *Frontiers in Psychology*, *14*

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Pronin, E., Lin, D. Y., & Ross, L. (2002). The Bias Blind Spot: perceptions of bias in self versus others. *Personality and Social Psychology Bulletin*, *28*(3), 369–381. https://doi.org/10.1177/0146167202286008

Hildebrandt, M. (2019). The issue of bias. The framing powers of ML. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3497597

BIBLIOGRAPHIC REFERENCES

Ehrlinger, J., Readinger, W., & Kim, B. (2016). Decision-Making and cognitive biases. In Elsevier eBooks (pp. 5–12). https://doi.org/10.1016/b978-0-12-397045-9.00206-8

Waldman, A. E., (September 18, 2019). Cognitive Biases, Dark Patterns, and the 'Privacy Paradox' 31 Current Issues in Psychology 2020, Available at SSRN: https://ssrn.com/abstract=3456155,

Mathur, A. et al. (2019) "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites," Lirias (KU Leuven), 3, Article 81, p. 6. Available at: https://lirias.kuleuven.be/handle/123456789/659030.

Grassl, P., Schraffenberger, H., Borgesius, F. Z., & Buijzen, M. (2020). Dark and bright patterns in cookie consent requests. Journal of Digital Social Research, 3(1), 1–38, p. 24, https://doi.org/10.31234/osf.io/gqs5h

Hoepman, J.-H. (2014) "Privacy Design Strategies," in IFIP advances in information and communication technology. Springer Science+Business Media, pp. 446–459, https://doi.org/10.1007/978-3-642-55415-5_38.

Bösch, C. et al. (2016) "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns," Proceedings on Privacy Enhancing Technologies, 2016(4), 237-254, https://doi.org/10.1515/popets-2016-0038.

Sax, M. (2021). Between empowerment and manipulation: The ethics and regulation of for-profit health apps. In Wolters Kluwer. https://pure.uva.nl/ws/files/58919538/Thesis.pdf

Luguri, J.B. and Strahilevitz, L. (2021) "Shining a Light on Dark Patterns," Journal of Legal Analysis, 13(1), pp. 43–109, Available at: https://doi.org/10.1093/jla/laaa006

Thaler, R. H., (2018), "Nudge, not sludge", Science, Vol. 361, Issue 6401, pp.431-431. Available at: DOI: 10.1126/science.aau9241

Hanson, J.D. and Kysar, D.A. (1999) "Taking Behavioralism seriously: Some evidence of market manipulation," Harvard Law Review, 112(7), 630-745,. Available at: https://doi.org/10.2307/1342413.

Calo, R. (2014) "Digital market manipulation", George Washington Law Review, Vol. 82., pp. 995-1051, Available at: https://digitalcommons.law.uw.edu/faculty-articles/25/

Di Geronimo, L. et al. (2020) UI dark patterns and where to find them, p. 5 Available at: https://doi.org/10.1145/3313831.3376600.

Santos, C., & Leiser, M. (2024). View of Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface. European Journal of Law and Technology, 15(1), https://ejlt.org/index.php/ejlt/article/view/990. https://ejlt.org/index.php/ejlt/article/view/990/1084

Malgieri, G. (2023). Vulnerability and Data Protection Law. In Oxford University Press eBooks. https://doi.org/10.1093/oso/9780192870339.001.0001

Mackenzie, C., Rogers, W., & Dodds, S. (2014). Introduction: what is vulnerability and why does it matter for moral theory? In C. Mackenzie, W. Rogers, & S. Dodds (Eds.), Vulnerability: new essays in ethics and feminist philosophy (pp. 1-29). Oxford University Press.)

Fineman, M. A. (2019). *Vulnerability and social justice*. Emory Law Scholarly Commons. https://scholarlycommons.law.emory.edu/faculty-articles/116/, 314-369

Rogers, W., Mackenzie, N., & Dodds, N. (2012). Why bioethics needs a concept of vulnerability. International Journal of Feminist Approaches to Bioethics, 5(2), 11-38, https://doi.org/10.2979/intjfemappbio.5.2.11

MacIntyre, A. C. (2001). Animales racionales y dependientes: Por qué los seres humanos necesitamos las virtudes, PP. 102-103, as cited by Masferrer, A., & García-Sánchez, E.

BIBLIOGRAPHIC REFERENCES

(2016). Vulnerability and human dignity in the age of rights. In Ius gentium (pp. 1–25). https://doi.org/10.1007/978-3-319-32693-1_1

Luna, F. (2018). Identifying and evaluating layers of vulnerability – a way forward. Developing World Bioethics, 19(2), 86–95. https://doi.org/10.1111/dewb.12206,

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building Understanding of the Domain of Consumer Vulnerability. Journal of Macromarketing, 25(2), 128-139, https://doi.org/10.1177/0276146705280622

Fuster, G. G. (2014). How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection. IDP Revista De Internet Derecho Y Política, 92-104, https://doi.org/10.7238/idp.v0i19.2424

Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. Computer Law & Security Review, 37, 105415. https://doi.org/10.1016/j.clsr.2020.105415

Masferrer, A., & García-Sánchez, E. (2016). Vulnerability and human dignity in the age of rights. In Ius gentium (pp. 1–25). https://doi.org/10.1007/978-3-319-32693-1_1

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. Philosophy & Technology, 29(4), 307–312. https://doi.org/10.1007/s13347-016-0220-8

Borberg, I. M., Hougaard, R., Rafnsson, W., & Kulyk, O. (2022). “So I Sold My Soul”: Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions, https://doi.org/10.14722/usec.2022.23026

Utz, C. Degeling, M., Fahl, S., Schaub, F., and Holz, T., (2019) (Un)informed Consent: Studying GDPR Consent Notices in the Field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212

Leiser, M., & Yang, W. (2022, November 12). Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive. https://doi.org/10.31235/osf.io/7dwuq

Leiser, M. (2024). Psychological Patterns and Article 5 of the AI Act: Deleted Journal, 1(1), 5–23. https://doi.org/10.21552/aire/2024/1/4

Häuselmann, A., & Custers, B. (2024). Substantive fairness in the GDPR: Fairness Elements for Article 5.1a GDPR. Computer Law & Security Review, 52, 105942. https://doi.org/10.1016/j.clsr.2024.105942

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected articles. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3839645

Malgieri, G. (2020). The Concept of fairness in the GDPR: A Linguistic and Contextual interpretation. *SSRN Electronic Journal*.

Santos, C., Rossi, A., *The emergence of dark patterns as a legal concept in case law.* (31 July 2023). Internet Policy Review. https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept.

Nikolaus, U. & Bohnert, S.: (2017) User Expectations vs. Web Design Patterns: User Expectations for the Location of Web Objects Revisited. Conference Proceedings after HFES Europe Annual Conference. https://www.hfes-europe.org/wp-content/uploads/2017/10/Nikolaus2017poster.pdf

Case Law

Case C-210-96, Gut Springenheide and Tusky (1998),

Case C-220/98, Estée Lauder Cosmetics GmbH & Co. OHG v. Lancaster Group GmbH (2000)

BIBLIOGRAPHIC REFERENCES

Case C-470/93, Verein gegen Unwesen in Handel und Gewerbe Köln e.V. v. Mars GmbH (1995)

Case C-122/10, Konsumentombudsmannen v. Ving Sverige AB (2011)

Pretty v. UK (29.04.2002), Application 2346/02;

Popshvili v. Belgium (13.12.2016), Application 41738/10.

Airey v. Ireland (9.10.1079), Application 6289/73

Yordanova v. Bulgaria, (05.06.2012), Application 25446/ 06

Dudgeons v. UK, (22.10.1981), Application 7525/76

Chapman v.UK, Application 27238/95 (18.01.2001)

M.S.S. v Belgium and Greece, (21.01.2011), Application 30696/ 09,

Ilias and Ahmed v. Hungary (21.11.2019), Application 47287/15

Z.A. and Others v. Russia (21.11.2019), Applications 61411/15, 61420/15, 61427/15 and 3028/16.

Kiyutin v Russia (10.03.2011), Application 2700/ 10

FTC v. Algoma Lumber Co.;

FTC v. Cyberspace.com, LLC (January 2008)

Brown Williamson Tobacco Corp. v. FTC (March 1983)

Federal Trade Commission v. Amazon.com (2023)

Federal Trade Comission v. Publishers Clearing House LLC (2023)

State of Texas v. General Motors LLC & OnStar LLC (August 2024)

EDPB Binding Decision 2/2023 (02.08.2023)

CNIL vs. Google LLC and Google Ireland Limited, (13.07.2023).

Datatilsynet vs. Grindr LLC (13.12.2021)

Italian Data Protection Authority's vs. Ediscom Sp.A, (February, 2023)

Other sources

Chatellier, R., Delcroix, G. Hary, E., et al., Shaping choices in the digital world - from dark patterns to data protection: the influence of ux/ui design on user empowerment, CNIL IP Reports - Innovation and Foresight, No. 6, 2019.

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

Consumer Protection: manipulative online practices found on 148 out of 399 online shops screened (30.01.2023) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.

Publications Office of the European Union. (2019). *The General Data Protection Regulation : report.* Publications Office of the EU. https://op.europa.eu/pt/publication-detail/-/publication/87d359d4-a83c-11e9-9d01-01aa75ed71a1

BIBLIOGRAPHIC REFERENCES

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 (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2805%29

EDPB Guidelines 4/2019, on Article 25 (Data Protection by Design and by Default), (20.10.2020), Available here: edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (europa.eu)

Consumer Vulnerability Across Key Markets in the European Union, (January 2016). Available on: https://commission.europa.eu/system/files/2018-04/consumers-approved-report_en.pdf

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

EDPB Guidelines 3/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

https://www.deceptive.design

https://dictionary.cambridge.org/dictionary/english/design

https://www.etymonline.com/word/design

Design Q & A: Charles and Ray Eames. https://www.hermanmiller.com/stories/why-magazine/design-q-and-a-charles-and-ray-eames/

What is design? (n.d.). International Council of Design. https://www.theicod.org/en/professional-design/what-is-design/what-is-design

Meggs, P. B. (2024). graphic design. Encyclopedia Britannica. https://www.britannica.com/art/graphic-design.

Lowgren, J. (2014). Interaction Design - brief intro. Interaction Design Foundation - IxDF. https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/interaction-design-brief-intro

Bandli, S. (2021) How the 8 design principles should be applied to learning. https://elearningindustry.com/how-apply-design-principles-to-online-learning.

CorelDRAW Graphics Suite | https://www.coreldraw.com/en/tips/graphic-design-principles/#principles.

Interaction Design Foundation - IxDF. (2016, August 30). What are the Gestalt Principles?. Interaction Design Foundation - IxDF. https://www.interaction-design.org/literature/topics/gestalt-principles

MSEd, K. C. (2024, April 22). What are the gestalt principles? Verywell Mind. https://www.verywellmind.com/gestalt-laws-of-perceptual-organization-2795835

Ludick, I. (2019, July 5). Design principles: Gestalt Psychology. https://www.linkedin.com/pulse/design-principles-gestalt-psychology-ian-ludick

Harley, A. (2023, March 6). The principle of common region: containers create groupings. Nielsen Norman Group. https://www.nngroup.com/articles/common-region/

Lumen Learning. (n.d.). Gestalt Principles of Perception | Introduction to Psychology. https://courses.lumenlearning.com/waymaker-psychology/chapter/gestalt-principles-of-perception/

BIBLIOGRAPHIC REFERENCES

Gaskin, J. (2024, June 13). What are gestalt design principles? A complete breakdown. Venngage. https://venngage.com/blog/gestalt-principles/#in

Wintermeier, N. (2023, February 7). Social Proof Examples: The Powerful Psychological Bias in Marketing. Crobox. https://blog.crobox.com/article/social-proof-examples

By the Power of Default. Center for Advanced Hindsight (2018, June 13). https://advanced-hindsight.com/blog/by-the-power-of-default/

Harris, T. (2019, October 16). How Technology is Hijacking Your Mind — from a Magician and Google Design Ethicist. Medium. https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3

Estefani, J. N. A. (2024, February 22). Designing With Integrity: The Ethical Designer's Handbook On Dark Patterns - Raw.Studio. Raw.Studio. https://raw.studio/blog/designing-with-integrity-the-ethical-designers-handbook-on-dark-patterns/

Rosala, M. (2024, January 30). Deceptive patterns in UX: How to recognize and Avoid them. Nielsen Norman Group. https://www.nngroup.com/articles/deceptive-patterns/

Flaherty, K. (2024, February 13). Evaluate Interface Learnability with Cognitive Walkthroughs. Nielsen Norman Group. https://www.nngroup.com/articles/cognitive-walkthroughs/

Together against deceptive design. (2023, June 6). Superbloom. https://superbloom.design/learning/blog/together-against-deceptive-design/