Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 127

Towards an Empowerment-Based Regulation of Dark Patterns: A Comparative Analysis of EU and US Law

Part 1 – Dark Patterns, Manipulation by Design

Fabien Lechevalier

2024

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Fabien Lechevalier is a Ph.D candidate in Law & Economics at Paris-Saclay University, France (CERDI). His research focuses on the collective dimension of the right to informational privacy, collective models of personal data governance and design research methods applied to law. With a multidisciplinary background, at the crossroads of law, economics and design, he is interested in research-action and research-creation approaches in the legal environment. He was a Visiting Fellow at the Digital Life Initiative at Cornell Tech and is a member of the NYU Privacy Research Group. He is a Lecturer in law at the Jean Monnet Faculty of Law - Economics & Management, Paris-Saclay University, and at the Mines-Telecom School of Engineering and Management (France). He currently co-pilots the Lab Surveillance, an experimental lab for legal research through design, supported by ENSCI Design School and Paris-Saclay University. He joined the TTLF as a TTLF Fellow in 2024.

General Note about the Content

This paper has been elaborated in collaboration with Amurabi & FairPatterns.

Suggested Citation

This TTLF Working Paper should be cited as:
Fabien Lechevalier, *Towards an Empowerment-Based Regulation of Dark Patterns: A Comparative Analysis of EU and US Law, Part 1 – Dark Patterns, Manipulation by Design*, Stanford-Vienna TTLF Working Paper No. 127, http://ttlf.stanford.edu.

Copyright

Abstract

Dark patterns or deceptive patterns can be defined as techniques of deception or manipulation of users through interfaces that substantially subvert or alter the autonomy, decision-making, or choices of a user during their online activities. These techniques are used, for example, to lead users to share more personal data, to pay higher prices for products or services, to prevent them from canceling subscriptions, or to make exercising their rights more difficult, if not impossible. The context in which these applications are used induces decision-making based on System 1 (Kahneman) and heuristics — quick and cognitively low-cost decisions. Law itself presents as the primary defense against these manipulative practices, which undermine trust in the digital space and the sustainability of the digital economy. While European legislators have established a relatively precise framework, across the Atlantic, in the United States, lawmakers appear to be more restrained. This initial study from the TTLF research project "Towards an Empowerment-Based Regulation of Dark Patterns" first aims to present these techniques of deception and manipulation, explain how they work, and why they are effective. We then seek to outline the regulatory framework governing dark patterns, both in Europe and the United States, while identifying its gaps. This study serves as a report on the first phase of the research project and is a state-of-the-art review.

Keywords

Dark patterns • Deceptive patterns • UX design • Behavioural economics • Cognitive bias • Law & economics • Legal design • Privacy law • Consumer protection law

TABLE OF CONTENTS

INTRODUCTION

[Aesthetics of Behavioral Manipulation] In recent years, a certain digital aesthetic has emerged, similar to the aesthetics found in architecture or decorative arts. Digital interfaces, like other art forms, contribute to our aesthetic relationship with the world. However, these new services are not aimed at art enthusiasts, but at consumers. This aesthetic, of which the user is often only dimly aware, subtly and substantially influences behavior through interface design[1], primarily for consumption purposes. These techniques are known as dark patterns or deceptive patterns[2]. They can be defined as deceptive or manipulative techniques within interfaces, designed to significantly subvert or alter a user's autonomy, decision-making, or choices in their online activities. While the term is relatively new, it would be wrong to say that interface design has only recently begun to manipulate our lives. Merchants have long influenced our purchasing behavior by shaping choice architectures[3]. For example, supermarkets have long arranged their layouts so that customer paths are guided by color codes or pre-established routes, aimed at maximizing purchases—from placing water packs at the far end of the store to displaying candy at the checkout. This is because, in the wake of the Bauhaus movement, design is grounded in a functional aesthetic aimed at solving problems, making commercial manipulation a natural application. The web giants have understood this well[4]. However, this new digital aesthetic of manipulation no longer garners the same approval, likely because it seems to exploit human

---

[1] In its broadest definition, interfaces could be defined as "shared spaces between different entities, systems, or sets whose material or perceptible characteristics allow them to exchange and interact through shared modes of representation", LINC-CNIL, 2019, p. 7.

[2] There is a rich body of scientific literature on the definition of dark patterns, with various taxonomies. See e.g. Mathur A. & al., 2021 ; Gray C. & al. 2018, pp. 1-14 ; Bongard-Blanchy K. & al., 2021 pp. 763-776 ; Maier M. & Harr R., 2020, p. 170. ; Waldman A. E., 2020, pp.105-109.

[3] See LINC-CNIL, 2019, p. 10.

[4] Ibid. , p. 1.

vulnerability and our tendency to become accustomed to forms that facilitate—at a high cost—our online experience.

[Protection Against Behavioral Manipulation] Beyond the direct consequences visible at the individual level, these practices raise broader questions about our collective relationship with technological progress and challenge our social contract in the digital age. In response to these new challenges, legislators have not remained mere spectators. Many laws in Europe, the United States, and elsewhere are already applicable to dark patterns. This new regulation of aggressive design falls within a broader movement toward recognizing neuro rights for citizens. Addressing neuro rights is always tricky because it involves a set of legal considerations that lie at the intersection of traditional law and neuroscience. Moreover, the boundaries with neuroethics are sometimes blurred, and some may even prefer the term neuro-ethical rights. Neuro rights, neuroethics, neuro-ethical rights—regardless of the terminology, the law is increasingly interested in the brain and its manipulation, to the point of constitutionalizing its protection. For example, in Chile, while a new constitution was being drafted, the 1980 Constitution was amended on October 25, 2021, to include the protection of mental integrity in a new paragraph in Article 19. According to the new text, resulting from Law 21,383, "Scientific and technological development shall be at the service of individuals and shall respect life and physical and mental integrity. The law shall regulate the requirements, conditions, and restrictions for its use on individuals, particularly protecting brain activity and the information derived from it". However, Chile is an exception. Although regulations exist, they are largely incomplete. This is partly due to lawmakers' limited understanding of observable practices, the law's limited intelligibility for the stakeholders involved, and regulators' limited capacity for action. In other words, the scope of regulation

through traditional legal frameworks is constrained. Thus, the law cannot act alone. Design also has a role to play.

[Plan] This research project, "Towards an Empowerment-Based Regulation of Dark Patterns", aims to bridge disciplines by advocating for better integration of design research, design practices, and designers into state regulatory strategies. However, this first working paper will focus on the state of the art. First, we aim to decrypt dark patterns. Dark patterns are a manifestation of the anarchic digital aesthetic. This anarchy results from the absence of rules, norms, or ethical constraints guiding the design of digital ecosystems. Until recently, designers were free to create without concern for the impact on users or society. This led to confusing or even harmful experiences that did not respect any hierarchy of values collectively agreed upon by the social digital contract. In essence, design anarchy reflects a process where form and function are no longer aligned. The form is dysfunctional, and the function is distorted. In this "anarchy", the core values of design, such as improving user experience and respecting individual autonomy, are subverted in favor of coercive and deceptive strategies. This "design anarchy" (1) weakens user trust, erodes their freedom of choice, and corrupts the ethical standards of the digital space, creating a competitive distortion where the most questionable practices are rewarded. In the absence of strict regulation, users are increasingly deprived of their decision-making power, reinforcing the asymmetry between them and companies and leading to a deterioration of the digital experience. The regulation that seeks to address this anarchy primarily relies on legal frameworks. Thus, we will then provide an overview of the applicable law, both in Europe and the United States, highlighting the limitations of this regulation (2). When addressed by law, the issue of dark patterns comes to the regulator's attention, marking the first step toward

a digital space that is more respectful of human limits. Moving from concrete law, which is ultimately limited, to ethics, which remains untapped, design emerges as a mediator. Between ethical action and ethics through design, between the regulation of design and regulation by design, a space for discussion emerges: neither fully within law nor entirely within design. Mapping the contours of this "no man's land" is one of the goals of this project, which will be explored in a second study.

1. *Dark patterns*, a design anarchy

"What kind of world will be born through the midwifery of our new and more powerful communications tools?"[5] This is the question posed by communications economist Dallas Smythe to post-war society in the 1950s. How are citizens affected by their digital environment? Does it empower them, limit their power, or merge both tendencies? While some believe that the digital technology universe guides us toward a society with almost mystical qualities, for others, it is anything but a space of empowerment[6]. Understanding these opposing claims requires a closer look at the role of individual, and by extension collective, agency in shaping the mediated environment, meaning the ability for users to make free and informed choices within it.

[5] Smythe D. W., 1950, p. 2.

[6] According to journalist Sylvia Zappi, "the expression refers to the process that allows individuals to become aware of their ability to act and to gain more power", Le Monde, 2013. This implies "the development of an individual's capacity for action, based on the ability to make rational, useful, effective, or intentional choices.", Bacqué M-H. & Biewener C., 2013, pp. 25-32.

1.1 Dark Patterns, interfaces exploiting social inequalities

1.1.1 Power Asymmetries

[Control Capitalism] In the digital age, contemporary capitalism is undergoing one of its most significant transformations. This new phase is driven not just by the rise of the Internet but, more importantly, by the dominance of digital platforms[7], which have become central to our lives through their constant capture of our attention[8]. Attention is now considered a scarce resource, with its scarcity located on the side of consumption rather than production. Traditionally, the economy focused on optimizing production with limited resources, but as Herbert A. Simon observed, we now live in an "attention economy"[9]. This attention is the foundation of a broader economy, which can be described as a control

[7] The Law No. 2016-1321 for a Digital Republic of October 7, 2016, provides, in Article 49 (now Article L111-7 of the Consumer Code), a legal definition of the concept of an online platform: "I.-An online platform operator is defined as any natural or legal person who, professionally, whether for profit or not, offers an online public communication service based on: 1° The ranking or referencing, through computer algorithms, of content, goods, or services offered or posted online by third parties; 2° Or the facilitation of interactions between several parties for the sale of a good, the provision of a service, or the exchange or sharing of content, goods, or services". For further developments, see Bacache-Beauvallet M. & Bourreau M., 2022.

[8] Simon H. A., 1971, pp. 37-72. For further developments, see Citton Y., 2014.

[9] This concept was introduced in 1971 by Herbert A. Simon, a future Nobel laureate in economics, who challenged the rationality of economic choices: "In a world rich in information, the abundance of information leads to a shortage of another resource: scarcity becomes what information consumes. What information consumes is quite obvious: it is the attention of its recipients. Thus, an abundance of information creates a scarcity of attention and the need to efficiently allocate this attention among the overabundance of information sources that can consume it".

economy. Political theorist Shoshana Zuboff terms this "surveillance capitalism"[10]. Unlike the totalitarianism of the Soviet era that inspired Orwell's *1984*, control capitalism relies on users voluntarily sharing more of their identities and desires to guide their choices or tailor content to their preferences[11]. The control and manipulation power of these platforms is made possible by the interfaces they design, which offer significant leeway in shaping user experience. Interfaces define the range of possible actions, subtly guiding or hindering certain behaviors, ultimately shaping user preferences[12]. This influence is magnified by platforms' vast, loyal audiences, making dark patterns—interface manipulations akin to nudging techniques—prevalent. Nudges, as defined by Richard Thaler and Cass Sunstein in their 2008 book *Nudge: Improving Decisions About Health, Wealth, and Happiness*[13], influence behavior without coercion, creating a system of "libertarian paternalism" where individuals are free to choose but subtly guided in a specific direction.

---

[10] It demonstrates that surveillance plays an unprecedented role in the creation of value today, but also that information, which is its product and structures exchanges, has itself become capital. At the very beginning of *The Age of Surveillance Capitalism*, Zuboff defines her object of study. What is surveillance capitalism? "1. A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; 2. A parasitic economic logic where the production of goods and services is subordinated to a new global architecture of behavior modification; 3. A distorted mutation of capitalism marked by unprecedented concentrations of wealth, knowledge, and power in human history; 4. The foundational structure of a surveillance economy; 5. A threat to human nature in the 21st century, as crucial as industrial capitalism was to the natural world in the 19th and 20th centuries; 6. The origin of a new instrumental power that asserts its domination over society and poses unprecedented challenges to market democracy; 7. A movement aimed at imposing a new collective order based on absolute certainty; 8. A dispossession of essential human rights, better understood as a top-down coup: a reversal of the sovereignty of the people.", Zuboff, Sh., 2020, p. 9.

[11] This is referred to as "behavioral targeting", a form of advertising that involves personalizing promotional content based on the online behavior of users and identifying their interests. For further developments., see Zuiderveen F. B., 2015.

[12] LINC-CNIL, 2019, p. 22.

[13] These authors define a "nudge" as "any aspect of the choice architecture that predictably alters people's behavior without forbidding any options or significantly changing their economic incentives. To qualify as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not coercive.", Thaler R. H., Sunstein C. R., 2010, p. 25.

[Take it or leave it] Alongside their direct influence over users, major platforms also exploit their central position in the digital ecosystem to become unavoidable standards in their sectors. Researchers note the illusion of choice when users face a "take it or leave it" ultimatum on these platforms. This worrying trend, both economically and democratically, stems from the abuse of market power by these platforms[14]. Over the past two decades, a handful of digital platforms have risen to dominate, often at the expense of users, creating monopolies that are difficult, if not impossible, to challenge without regulatory intervention. In any market, users' main power is their freedom to choose whether to use a service or report abuses to the authorities. However, the power asymmetry also manifests in a lack of effective competition, leaving users without satisfactory alternatives. In perfectly competitive markets, many companies compete to attract consumers, keeping prices close to production costs while innovation and service quality are driven by competition. In contrast, monopolies and oligopolies, due to their substantial market power, can raise costs without fear of backlash from consumers or competitors. Dominant platforms can lower service quality without losing customers since viable alternatives are often non-existent or unsatisfactory. This lack of choice and effective competition leads to a deterioration of service conditions, as platforms have little incentive to improve standards or interfaces. Today, individual agency is reduced to either accepting the terms imposed by tech giants or opting out of the digital sphere entirely.

[14] See e.g. Bar-Gill O., 2012.

1.1.2 Information Asymmetries

[The Role of Information] The ability of digital service users to make free choices appears even less feasible given that their relationships with platforms are characterized by significant informational asymmetries. These refer to situations where market actors do not have access to the same information, whether it concerns the quality of the product being exchanged, the risks to which users are exposed, or the behavior of each party in a transaction. To illustrate this theory, one can think of a borrower who knows better than the lender their ability to repay, or of an insurance policyholder who knows better than the insurer the potential risks they face. Akerlof (awarded the Nobel Prize in Economics in 2001) favored the example of the used car market ("lemons"), where the seller knows more about the quality of the car than the buyer[15]. Since the 1970s, economists have increasingly focused on markets with informational asymmetries, particularly those where a consumer has difficulty assessing the quality of the products or services involved in transactions. These economists believe that such informational asymmetries can lead to market failures[16]. Dark patterns exploit and reinforce these informational asymmetries. The exploitation of these asymmetries through dark patterns can reduce consumer welfare by pushing them to make choices that do not maximize their utility. Dark patterns reduce the necessary information consumers need to perform transactions that maximize their utility in three ways:

- **Omitting Crucial Information**: For example, a "free trial" offer may conceal an automatically renewing paid subscription, which becomes difficult or even impossible to cancel after the trial period ends. This type of dark pattern, known as the "roach motel"

[15] Akerlof G., 1970.

[16] Ibid.

according to Harry Brignull's taxonomy[17], falls under the "obstruction" category in the preliminary ontology developed by Gray, Santos, and Bielova[18]. In this case, dark patterns hide the real costs of a product or service by omitting key information until the final stages of the transaction. This undermines price transparency, a fundamental principle for proper market functioning, and can lead consumers to make suboptimal choices.

- **Making Information Hard to Find or Understand**: An example is the use of long, jargon-filled privacy policies that obscure important details or present contradictory information. This type of dark pattern is referred to as "left in the dark" in the taxonomy developed by the European Data Protection Committee in 2023[19]. Interfaces are designed to hide information or data protection controls, leaving users uncertain about how their data is handled or the extent of control they have over it. By making information difficult to access or presenting it in a confusing manner, these dark patterns increase transaction costs for consumers. These costs include the time and effort required to locate relevant information, understand it, and compare various options. This complexity can discourage users and lead them to make decisions that do not maximize their utility. In the following section, we further explain the role and function of transaction costs.
- **Presenting Misleading Information**: For instance, emotional manipulation is used when a button to decline an offer is phrased to make the user feel guilty or foolish: "No thanks, I don't want to look my best", while the brightly colored "Buy Now" button stands out in the checkout process. This type of dark pattern, known as "confirmshaming", influences

[17] Brignull H., blog.

[18] See Gray C., Santos C. & Bielova N., 2023, p. 4.

[19] See EDPB, 2023.

user decisions by triggering uncomfortable emotions like shame. Efficient market allocation relies on consumers making informed decisions based on an accurate evaluation of the costs and benefits of available options. However, dark patterns compromise this process by distorting user decision-making through lack of transparency, leading consumers to purchase products or services that do not maximize their utility. They may also underuse more advantageous options that are not presented fairly or prominently.

[Transaction Costs] The role of the law is therefore to attempt to address informational asymmetries by protecting consumers as much as possible. The natural reaction of lawmakers, at first, was to increase the amount of information made available to users of digital services, aiming to enable them to make more free and informed choices. However, this strategy has created new problems, notably the increase in transaction costs, which can paradoxically contribute to the persistence of informational asymmetries. Transaction costs represent all the costs involved in a market exchange between two economic agents to complete the exchange[20]. These may include the costs of searching for and evaluating a service or feature, information costs, verifying the terms of a service, drafting an email, etc. The time required for consumers to inform themselves is also a transaction cost. Behavioral economics literature has widely demonstrated that consumers do not read non-critical, yet essential information such as terms of service, privacy policies, or even the descriptive text of "mandatory checkboxes". Since consumers do not read this information, it can be inferred that the transaction cost involved in doing so is too high. This reinforces the informational

[20] See Coase R., 1937. Transaction costs are not a market failure, but they help explain why the problem of information asymmetry is difficult to solve. See Dahlman C. J., 1979.

asymmetry[21]. There are several reasons why users do not read this information. These include the time it takes to do so[22], as well as the complexity of the language and terms used[23]. Seeking or using another, more respectful service may seem like a viable solution, but it also poses a problem because it implies another form of transaction cost[24]. When these costs are high, consumers are less likely to search for alternatives, reducing competition in the market. Interface design strategically uses transaction costs to modify user behavior. However, even if users took the time to read and tried to understand the information presented — in other words, even if they considered the transaction cost justified — they would still lack the cognitive ability, given the design of the interfaces, to make an informed decision. For example, they are unable to assign a monetary value to the information about their behavior or to calculate the probabilities of future events resulting from their current behavior[25]. Individuals' choices are thus limited, not only by the amount of information they have at the time of making a decision (such as accepting, clicking, or checking a box), but also, as we will now demonstrate, by the cognitive capacities they have to make these decisions within a limited timeframe.

---

[21] See e.g. Faure M. G. & Luth H. A., 2011, p. 342 ; Wagner G., 2010, p. 61-62 ; Schäfer H. B. & Leyens P., 2010, p. 105, p. 108.

[22] For example, Cranor & McDonald calculated that it would take an average American 244 hours per year to read the privacy policies of the websites they visit. This would amount to about forty minutes per day, roughly half of the time the average American spent online each day (in 2006). Expressed in monetary terms, this cost would be around $781 billion in lost productivity and wasted time, if people were to read privacy policies. The costs to individuals to stay informed would exceed the revenue of the advertising industry. All online advertising revenues in the U.S. were estimated at $21 billion in 2007. See Cranor L. F. & McDonald A. M., 2008.

[23] Privacy policies are often long and difficult to read. In one study, more than half of the privacy policies examined were too difficult for most Americans to understand (Jensen C. & Potts C., 2004). A quarter of Europeans believe privacy policies are too difficult. (See European Commission (Eurobarometer), 2011, pp. 112-114). Finally, privacy policies are often vague and lack transparency about data processing practices. Verhelst E. W., 2012, p. 221.

[24] For instance, transferring emails and contacts to a more privacy-conscious email provider can be time-consuming. On this point., see Shapiro C. & Varian H. R., 1999, p. 104.

[25] Acquisti A. & Grossklags J., 2007, p. 365.

1.2 Dark patterns, interfaces exploiting cognitive inequities

1.2.1 The limits of human rationality

[Perfect Rationality, Economic Approach] Faced with complex choices, some of whose parameters are difficult or impossible to calculate, and given the available information and time, a user of a mobile service must settle for making a "reasonable" choice. Classical economic theory considers this to be a rational and optimal choice. This concept refers to *homo economicus*, an individual who acts in a perfectly rational manner based on their interests and objectives. The term seems to have emerged in the second half of the 19th century, coined by John Stuart Mill in his *Principles of Political Economy* (1848) and later taken up by Vilfredo Pareto in his *Manual of Political Economy* in 1906[26]. According to this theory, users are expected to maximize their utility intertemporally by using all available information and acting consistently with their preferences while assessing future damages in relation to their probability of occurrence. To make these decisions, users make a trade-off between the net benefits gained from the transaction mediated by the interface and those associated with rejecting it (such as preserving privacy or financial resources). In economic terms, this is called a cost-benefit analysis, which means comparing the cost of a decision with its benefits. However, the perfect rationality approach encounters significant limitations, as demonstrated by Alessandro Acquisti[27]. First, information is not perfect, as we have seen,

[26] He defended it: "Rational mechanics, when it reduces bodies to mere material points, and pure economics, when it reduces real people to *homo economicus*, both rely on perfectly similar abstractions.", Pareto V., 1963, p.17.

[27] Acquisti A., 2004, pp. 21-29.

but more importantly, individuals' cognitive capacity is even more limited. In reality, making a "reasonable" choice forces individuals to rely on simple heuristic procedures to reach solutions more quickly and with less effort. For example, a person may rationally imitate the behavior of their peers when it comes to online privacy protection to avoid the costs of calculating such decisions. If no one adopts protective measures, they will not either[28]. In doing so, individuals face their own psychological distortions and cognitive biases, which turn what seems like a reasonable choice into an irrational one.

[Bounded Rationality, Behavioral Approach] The concept of cognitive biases was introduced in the 1970s by Daniel Kahneman and Amos Tversky to explain certain irrational decisions in economics[29]. These new behavioral economists continued the work on bounded rationality initiated by institutional economics scholars, particularly Herbert A. Simon[30]. As early as 1947, Simon questioned the model of *homo economicus*. He rejected the components of classical decision theory and developed the concept of bounded rationality. Herbert A. Simon occupies a central place for the influence that his theory of "bounded rationality" has exerted. Inspired by the work of psychologist George Katona, considered a precursor to behavioral economics, Simon was one of the first to advocate for a behavioral approach to economics, which relies heavily on psychology. According to Simon, based on psychological studies, individuals do not optimize; they make decisions when they appear to be "satisficing"[31]. This term, coined by Simon, refers both to the decision-making process, which is trial and error depending on the context, and to the outcome of this process, which

[28] Rochelandet F., 2010, p. 83.

[29] Kahneman D. & Tversky A., 1979, pp. 263-292.

[30] Simon H. A., 1947 ; March J. G., 1958 ; Hosseini H., 2003.

[31] Simon A. H., 1959, pp. 262-263.

may deviate from what classical theory defines as optimal. Cognitive biases are closely related to System 1, theorized by Daniel Kahneman[32], because they are used to make quick decisions. They act as a kind of "mental shortcut", an irrational and systematic pattern that influences judgment and decision-making. For Kahneman, our brain, particularly the prefrontal cortex, uses two main strategies for decision-making. System 1 is fast, efficient, and requires little cognitive effort, but it is not always accurate. In contrast, System 2 is slower and more analytical, requiring significant cognitive effort but generally leading to more accurate solutions. System 3 then acts as an arbitration mechanism, interrupting System 1 when necessary to activate the more reliable algorithms of System 2. Cognitive biases can, in some cases, allow for faster and more efficient decision-making because they reduce the amount of information needed to make a decision and simplify the judgment process. However, the problem with cognitive biases is that they are based on inputs that are not objective, which can lead to irrational decisions. Moreover, they are systematic, replicable, difficult to suppress, and operate silently (i.e., we are not aware of the factors influencing our decisions). Thus, cognitive biases are a form of unconscious errors in the decision-making process that can lead to incorrect conclusions or irrational interpretations. Because they are systematic, cognitive biases make human decisions predictable and, therefore, exploitable or even manipulable. Dark patterns take advantage of these flaws in the human brain to induce behaviors that individuals would not have consciously chosen.

[32] See Kahneman D, 2011.

1.2.2 The exploitation of human cognitive biases

[Cognitive Biases, Mapping] More than 180 cognitive biases have been identified in the literature, and they can be categorized into four main groups: biases related to cognitive overload, biases arising from a lack of meaning, biases caused by the need for quick reactions, and biases linked to information that must be remembered for later.

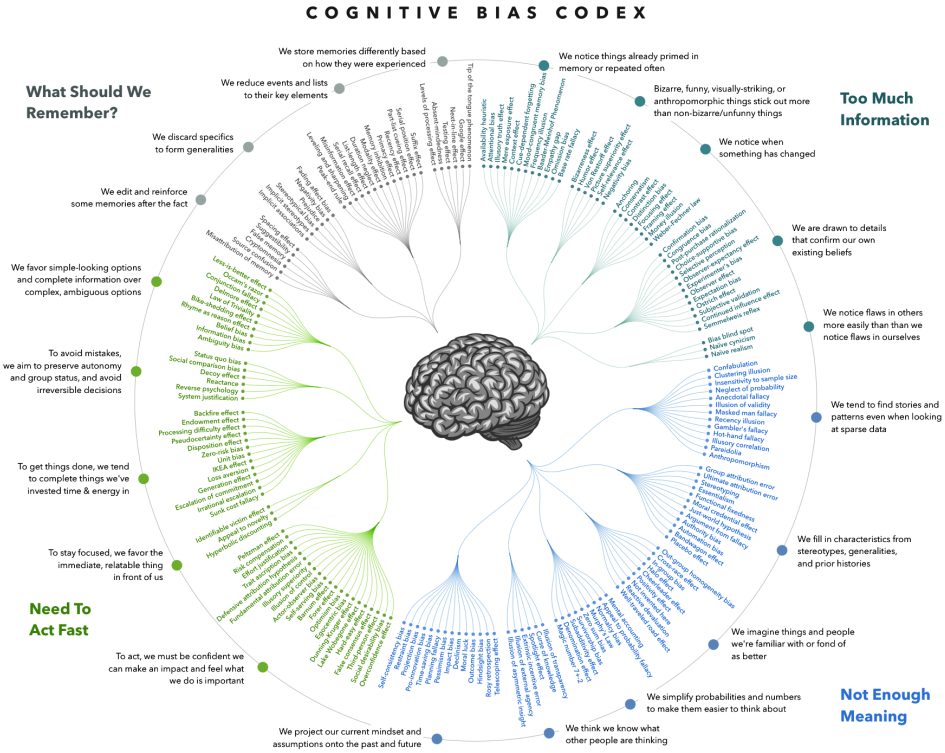

Fig. 1. Codex, Manoogian III J. & Buster B., 2016.

Several authors have identified the key cognitive biases that dark patterns exploit[33]:

- **Anchoring effect**: The tendency to rely on the first piece of information received, which influences subsequent decisions. This bias is at play in dark patterns such as "false hierarchy", where an option is presented as the "best deal" ;

[33] See e.g. Waldman A. E., 2020 ; Jarovsky L., 2022 ; etc.

- **Framing effect**: The way information is presented influences our decisions. This bias is heavily exploited in dark patterns like "confirmshaming" or "sneak into basket " ;

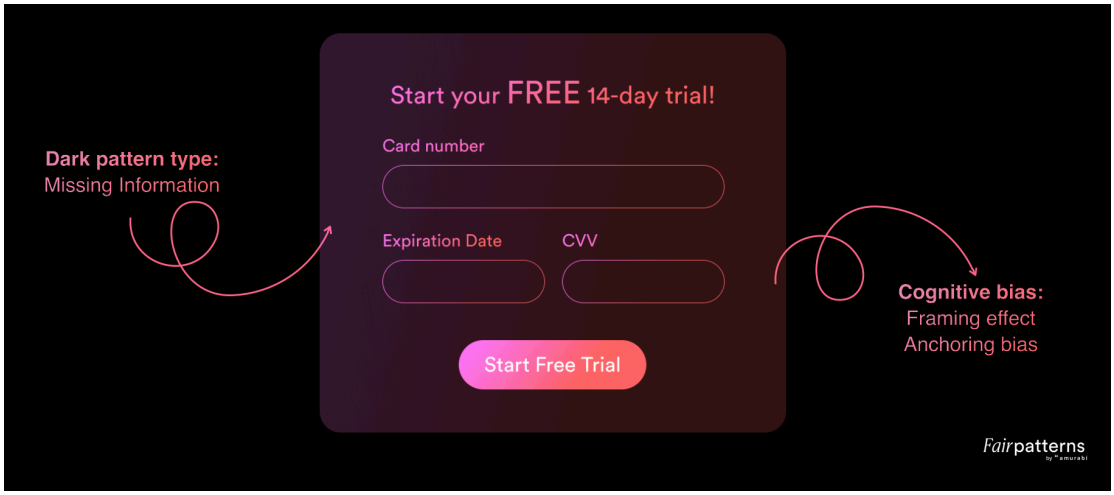

Fig. 2. ***Dark pattern*** **; type** ***Missing information***

- **Default choice effect**: The tendency to accept a preset option without questioning it, regardless of personal preferences. This bias is extensively used in checkboxes ;

- **Optimism bias**: When in a positive emotional state, an individual overestimates the likelihood of favorable outcomes and underestimates risks, assuming they are less exposed to them than others in similar situations. This bias is exploited in dark patterns like "false hierarchy", where the "Accept All" button is made more prominent than the "reject all" option or link ;

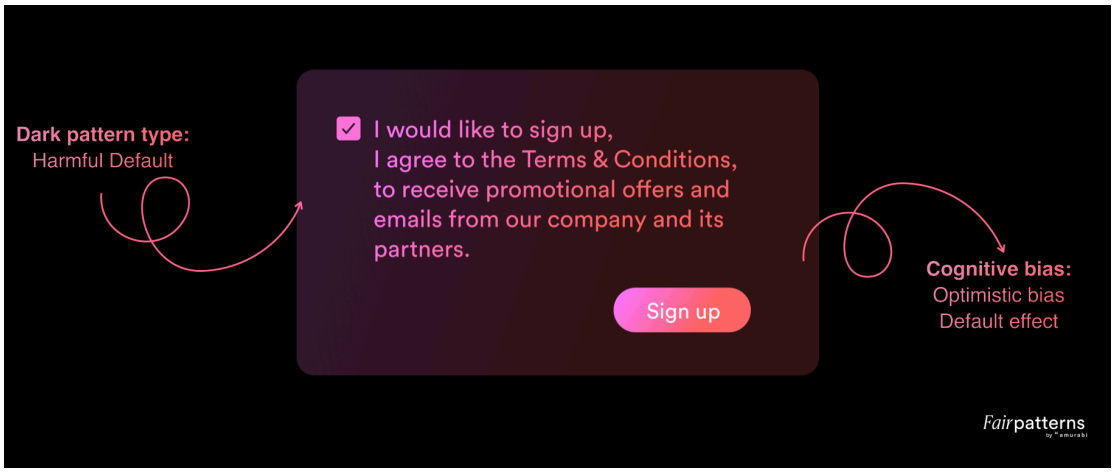

Fig. 3. ***Dark pattern*** **; type** ***Harmful Default***

- **Hyperbolic discounting effect**: The preference for immediate rewards over long-term benefits. This bias is exploited in dark patterns that play on emotions (e.g., “stirring”): "allow your friends to know where you are at all times", without considering long-term consequences like tracking by the app ;
- **Overchoice effect**: The tendency to be unable to make decisions when confronted with too many options. This bias is exploited in dark patterns like the "privacy maze", where users effectively give up control over their data when overwhelmed with too many checkboxes.

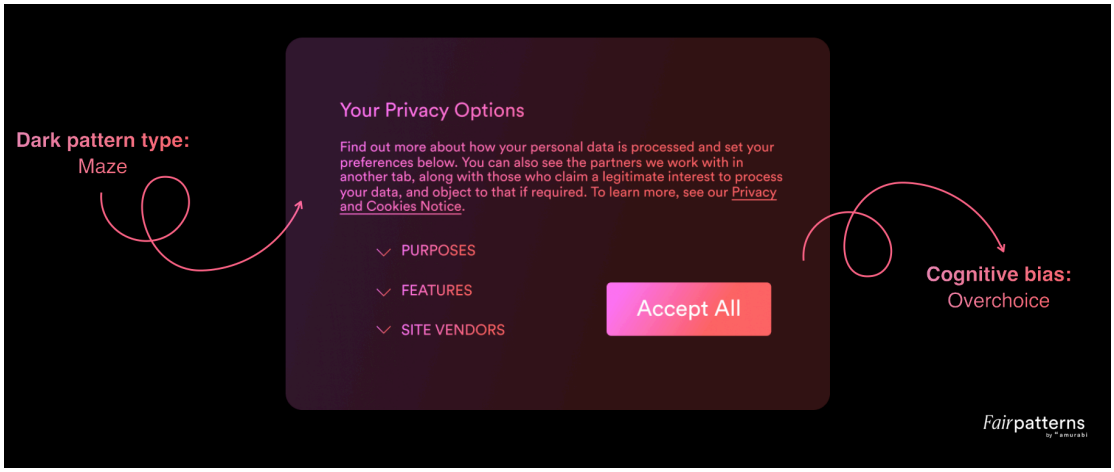

Fig. 4. *Dark pattern* ; type *Maze*

[Cognitive Biases, Consequences] Numerous studies show that most users cannot avoid dark patterns, even in the rare cases when they recognize them[34]. These techniques are particularly "effective" on mobile apps, where screen size further intensifies cognitive biases and makes them even harder to resist[35]. Researchers, therefore, consider dark patterns a form of online manipulation, depriving users of their ability to make autonomous and informed

[34] See e.g. Bongard-Blanchy K. & al, 2021 ; Waldman A. E., 2020 ; Jarovsky L., 2022.

[35] See e.g. Gunawan J. & al., 2021 ; Di Geronimo L. & al., 2020 ; Maier & Harr, 2020.

decisions[36]. Maier and Harr, for example, identified that users are "moderately aware of these deceptive techniques" and largely "resigned" to them[37]. Moreover, many authors have highlighted that the metacognitive decision-making process impairs individuals' ability to make choices that truly reflect their preferences. Faced with a difficult choice, signaling significant difficulty or even impossibility, users tend to give up. For example, Waldman concludes that the more difficult users find it to make choices regarding their personal data while browsing, the more likely they are to give up on protecting their data[38]. The exploitation of these cognitive biases, these flaws in our rationality that hinder our free decision-making capacity, is one of the fundamental drivers in the race for capturing internet users' attention. In the end, dark patterns represent a modern exploitation of our cognitive biases through interfaces. Beyond the direct individual-level consequences, these techniques challenge our collective relationship with technological progress and question our social contract in the digital age. Faced with these new challenges, the legislator is not merely a passive observer.

[36] Susser D., Roessler B., & Nissenbaum H. F., 2019.

[37] Maier M. & Harr R., 2020, p. 190.

[38] Waldman A. E., 2020.

2. *Dark patterns*, a design regulation

Law presents itself as the primary bulwark against online behavioral manipulation practices that undermine trust in the digital space and the sustainability of the digital economy. In Europe, legislators have not hesitated to directly address dark patterns, first by naming them and then by broadly prohibiting their use. On the other side of the Atlantic, in the United States, the legislative response has been more measured. The adoption of the new California Consumer Privacy Act in 2020, made California the first state to ban the use of dark patterns by digital interface designers. However, the scope of the California law, as well as other national or federal regulations, appears more limited. The concept of dark patterns is multifaceted, flexible, and adaptable. To tackle it, one must first understand it, a task that is not so simple for legal practitioners.

2.1 In Europe

While numerous European-level laws already apply to dark patterns, treating them as unfair practices that violate data protection laws, abuse of dominance prohibitions, or specific sectoral regulations[39], new laws have recently been enacted to explicitly ban them as "dark patterns". Fundamental regimes have been updated and supplemented by new secondary laws, which, due to their novelty, contain provisions that explicitly reference dark patterns:

The general provisions are supplemented by numerous sector-specific texts. The e-Commerce Directive 2000/31/EC requires that commercial information be easily accessible and presented in a clear and unambiguous manner, opposing dark patterns such as "hidden information". The Audiovisual Media Services Directive 2010/13/EU, as amended by Directive 2018/1808, mandates that all advertising be clearly identifiable as such and prohibits the use of subliminal techniques, countering dark patterns such as "disguised ads". This study will not go into detail on the sector-specific texts but rather aims to provide a general overview.

the *Digital Markets Act* and the *Digital Services Act* on the one hand, and the *AI Act* on the other. Consequently, it is important to note that these new laws will only apply to dark patterns if they are not already prohibited by existing regulations.

2.1.1 General legislation

[Consumer Law] In EU law, Directive 2005/29/EC on Unfair Commercial Practices (UCPD)[40] governs business-to-consumer (B2C) relations, prohibiting practices deemed unfair. Dark patterns, as techniques of manipulation and deception, fall within the scope of the UCPD and can therefore be challenged under this framework.

Directive 2005/29/EC, May 11, 2005, on Unfair Commercial Practices (UCPD)

The directive applies to all promotion, sale, or provision of products or services to consumers, regardless of where the trader is established. The trader can be a natural or legal person, including charitable organizations or public authorities when they engage in commercial activities[41]. A commercial practice can be an action, omission, or marketing communication, whether before, during, or after a transaction. It is considered unfair if it can influence a transactional decision that the consumer would not have otherwise made. These decisions include not only purchases but also related choices, such as entering a store[42]. Unfair practices breach the trader's professional

---

[40] EP and Council of the EU, Directive 2005/29/EC, May 11, 2005, concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC and 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).

[41] UCPD, Article 2.

[42] ECJ, C-281/12 Trento Sviluppo srl, §35.

diligence[43] and can be misleading (by action or omission)[44] or aggressive[45]. Misleading practices conceal or distort information, while aggressive practices involve harassment or coercion. There is no need for the intent to deceive for a practice to be deemed unfair. Authorities first check if the practice is listed in Annex I of the directive; if not, they assess it on a case-by-case basis, determining whether it could lead consumers to make undesirable transactional decisions. Practices are evaluated from the perspective of the average consumer, who is "reasonably well-informed, observant, and circumspect"[46]. For vulnerable consumers, such as children or the elderly, the assessment is made from their specific perspective, taking into account their particular characteristics or context[47]. For instance, practices targeting children are evaluated based on how children process information differently. The UCPD applies both online and offline[48].

The 2021 Guidelines issued by the European Commission provided more clarity by specifically addressing the application of the directive to digital environments[49]. B2C practices, even without direct payment but generating benefits for the merchant, such as data monetization, are covered. The guidelines dedicate a section to dark patterns, stating that they can be contested under the UCPD. Annex 1 directly prohibits certain dark patterns, such as "bait and switch", "false limited stock", "fake countdown timers", and "harassment". Other dark patterns may be deemed deceptive if they hide information or mislead, or aggressive if

---

[43] UCPD, Article 5.

[44] UCPD, Article 6 & 7.

[45] UCPD, Article 8 & 9.

[46] ECJ, C-210/96 Gut Springenheide & Tusky, §31.

[47] European Commission, 2021, p. 35.

[48] ACM, 2022, p.15.

[49] European Commission, 2021.

they impair freedom of choice through coercion or undue influence. For example, making it harder to cancel a contract than to enter one or hiding unavoidable booking fees are considered deceptive practices prohibited by the UCPD. Finally, the Unfair Commercial Practices Directive has been complemented by Directive 2011/83/EU on consumer rights[50], which specifically addresses dark patterns such as "consumer-unfriendly default settings"[51] and "hidden costs"[52]. It is also complemented by Directive 93/13/EEC on unfair contract terms[53], which protects consumers from unfair, individually non-negotiated contract clauses. A contract may be annulled if its terms are presented unclearly, using deceptive interfaces to confuse consumers with visual interference. As such, the directive on unfair contract terms applies more specifically to dark patterns like "information overload" (i.e., unintelligible walls of text) or "trick questions" (e.g., double negatives or text that contradicts the interface's suggestions).

[Competition Law] In a liberal market economy, competition law plays a central role in protecting the market from anticompetitive behavior by companies. It aims to limit the negative manifestations of market power that distort competition and harm consumers. As previously discussed, the quasi-monopoly of major platforms allows them to lower service quality without fearing significant customer loss due to a lack of viable alternatives. The absence of real competition leads to a general degradation of standards and interfaces. Dark patterns could thus harm consumers in relation to the prohibition of abuse of dominant

[50] EP and Council of the EU, Directive 2011/83/EU, October 25, 2011, on Consumer Rights.

[51] Ibid., Article 22.

[52] Ibid., Recital 27.

[53] EP and Council of the EU, Directive 93/13/EEC, April 5, 1993, on Unfair Terms in Consumer Contracts.

position as outlined in Article 102 of the TFEU[54]. Therefore, one can imagine that the directive could be indirectly applicable.

✚ Treaty on the Functioning of the European Union, October 26, 2012 (TFEU)

Article 102 TFEU concerns the unilateral behavior of companies in a dominant position in a specific market. Market power itself is not problematic, but the dominant company has a special responsibility not to abuse this power[55]. Article 102 TFEU lists non-exhaustive examples of abusive practices[56], distinguishing between two types of abuse: exploitative abuse and exclusionary abuse. Exploitative abuse includes actions that directly exploit customers and consumers, such as excessive pricing. Exclusionary abuse involves artificially erecting barriers to market entry and expansion, thus excluding competitors. Recent developments in digital competition have given rise to a new generation of hybrid cases exhibiting characteristics of both types of abuse. Under Article 102 TFEU, dark patterns could become a tool for anticompetitive exclusionary behavior[57]. For example, academic literature has shown that dark patterns such as "roach motels" lead to high switching costs for consumers and even hinder their choices, artificially creating advantages for the dominant company[58]. Examples include default choices (pre-selection) and information framing that impact consumer decision-making, potentially allowing dominant firms to engage in problematic self-preferencing behavior. It is important to note that when different dark patterns are deployed

---

[54] EP and Council of the EU, Treaty 2012/C 326/01, October 26, 2012, Treaty on the Functioning of the European Union, Article 102.

[55] ECJ, 1983, C-322/81 Nederlandsche Banden Industrie Michelin (Michelin I), §57.

[56] ECJ,1973, C-6-72 Europemballage Corporation and Continental Can Company Inc., §26.

[57] Morozovaite, V., 2023, p. 410.

[58] European Union Commission, 2022, p. 91 ; ICO, CMA and DRCF, 2023, p. 10.

> systematically on a large scale, the cumulative effects could weaken or distort competition and reduce incentives to innovate for the benefit of consumers. Moreover, manipulating consumers on a large scale may constitute exploitative abuse, as the aim of such practices is to extract as much consumer surplus as possible[59].

Thus, it seems that certain dark patterns could be considered an abuse of dominant position. Competition law would then support the action of unfair commercial practices law. For example, the European Commission sanctioned Google for abuse of dominance through its search engine by promoting its own comparison shopping service in a way that favored it. This practice combined dark patterns such as "obstructing comparison", "favoring", and "defaults". If the conditions for abuse are met, these practices could therefore be deemed abusive, with penalties of up to 10% of the global turnover of the dominant companies.

[Data Protection Law] The use of dark patterns also raises concerns under data protection regulations. By imposing principles of transparency, fairness in processing, and data minimization, the General Data Protection Regulation (GDPR)[60] generally opposes all dark patterns that lead users to share more data than they would consciously choose to (e.g., "Privacy Zuckering", "Emotional Stirring"), or those designed to create confusion about data use or user rights (e.g., "Privacy Maze", "Information Overload", "Trick Questions »).

[59] Graef, I., 2023.

[60] EP and Council of the EU, Reg. 2016/679, April 27, 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, known as GDPR).

✚ Regulation 2016/679, April 27, 2016, concerning the protection of natural persons regarding the processing of personal data and the free movement of such data (GDPR)

The GDPR established a European framework for personal data protection, defined as "any information relating to an identified or identifiable natural person"[61]. It applies to any data processing by entities offering goods or services to individuals in the EU or monitoring their behavior, regardless of location[62]. The Regulation grants individuals rights over their data, including information and control over its processing[63]. Article 5(1)(a)(c) requires processing to be fair and based on one of the six legitimate grounds listed in Article 6(1)[64]. Article 5(2) mandates transparency, data minimization, and accountability[65]. One of the legitimate grounds for processing is consent, which must be "freely given, specific, informed, and unambiguous"[66]. Article 12 requires that information be "concise, transparent, intelligible, and easily accessible"[67]. However, some user interfaces make it difficult to provide free and valid consent, violating Articles 4(1) and 5[68]. To prevent such practices, the GDPR prohibits misleading online interfaces that push users to accept more data processing than is in their best interest[69]. The CJEU, for example, ruled that a pre-checked box does not constitute valid

[61] GDPR, Article 4(1).

[62] GDPR, Article 3.

[63] GDPR, Article 12 to 22. These Articles describe the rights of data subjects, in particular with regard to information and control of the processing of their personal data.

[64] GDPR, Article 5(1)(a)(c).

[65] GDPR, Article 5(2).

[66] GDPR, Article 4(11).

[67] GDPR, Article 12.

[68] Sinders, 2021; European Commission, 2021.

[69] Luguri & Strahilevitz, 2021.

consent[70], and that "yes" and "no" options in a cookie form must be equally accessible[71].

To clarify the GDPR's scope, the European Data Protection Board (EDPB) adopted guidelines in February 2023[72] under Article 60 of the GDPR[73]. These guidelines provide practical recommendations for social media platform designers and users on how to evaluate and avoid dark patterns in social media interfaces that violate GDPR requirements. The EDPB defines dark patterns as "user interfaces and experiences implemented on social media platforms that lead users to make involuntary, unwanted, and potentially harmful decisions regarding the processing of their personal data". The guidelines give concrete examples of dark patterns, outline best practices for various use cases, and offer specific recommendations for UI designers to facilitate GDPR-compliant implementation. They detail six categories of dark patterns: "Overloading" (too much information), "Skipping" (making users overlook privacy aspects), "Stirring" (using emotions to influence decisions), "Hindering" (making data management difficult), "Fickle" (confusing interfaces), and "Left in the dark" (hiding important information). According to the EDPB, these six categories can be grouped into patterns based on content or interface design. The former pertains to the information content, including wording, context, and informational components, while the latter refers to how content is visually presented and how users interact with it. The guidelines are structured around the five stages of a social media user account's life cycle: (1) opening an account, (2)

---

[70] ECJ, 2019, C-673/17 Planet49 GmbH.

[71] ECJ, 2020, C-61/19 Orange Romania, §53.

[72] European Data Protection Board, 2023.

[73] The drafting of such guidance is part of the EDPB Strategy and Work Programme 2021-2022 to support effective enforcement and efficient cooperation between national supervisory authorities (SAs). The guidelines provide a detailed description of the GDPR cooperation between SAs and aim to further increase the consistent application of the legal provisions relating to the one-stop-shop mechanism. The guidelines help SAs to interpret and apply their own national procedures in such a way that it conforms to and fits in the cooperation under the one-stop-shop mechanism.

staying informed on the platform, (3) staying protected on the platform, (4) exercising personal data rights, and (5) leaving the platform. Finally, in addition to the GDPR, Article 5(3) of the e-Privacy Directive 2002/58/EC[74] emphasizes that when consumers must consent to cookies, misleading interfaces can undermine legitimate consent[75]. Thus, it opposes dark patterns that make the "I accept" button more accessible than "I refuse" or "I manage settings", or that create confusion between the text and the associated button. Similarly, Article 4(4) of the Data Act[76] prohibits data holders from making it unduly difficult for users to make choices or exercise rights under the Regulation[77].

2.1.2 Specific legislation

[Regulation of Digital Platforms] For forty years, competition law, consumer law, and data protection have been the primary instruments through which the European Union has developed a regulatory framework for digital technologies and services. In recent years, these fundamental regimes have been updated and supplemented by new secondary legislation that, due to its novelty, contains provisions explicitly referencing dark patterns: the Digital Markets Act (DMA) and the Digital Services Act (DSA)[78]. The European regulation

---

[74] EP and Council of the EU, Directive 2002/58/EC, July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, known as the e-Privacy Directive), Article 5(3).

[75] European Commission, 2022, p. 75

[76] EP and Council of the EU, Reg. 2023/2854, December 13, 2023, on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[77] Data Act, Article 4(4), "Data holders shall not make the exercise of choices or rights under this Article 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 ".

[78] EP and Council of the EU, Reg. 2022/2065, October 19, 2022, on a single market for digital services (Digital Services Act, known as the DSA), amending Directive (EU) 2000/31/EC.

on digital services (DSA), one of the EU's major digital initiatives along with the regulation on digital markets (DMA)[79], explicitly prohibits dark patterns for the first time in Europe in binding legislation. Indeed, Article 13 of the DMA includes an "anti-circumvention" provision targeting key prohibitions imposed on "gatekeepers" (mainly the GAFAM companies) through "interface design". However, it is the DSA that explicitly bans these techniques. The DSA regulates the provision of intermediary online services within the EU. Article 25 prohibits the use of deceptive or manipulative online interfaces by platforms, a term which, as Recital 67 illustrates, encompasses dark patterns. This prohibition was absent from the initial Commission proposal but was added by the Council and Parliament during trilogue negotiations[80].

+ Regulation 2022/2065, October 19, 2022, concerning a Digital Services Internal Market (DSA)

Under the rubric "online interface design and organisation", Article 25(1) DSA prohibits online platforms from "design[ing], organi[sing], or operat[ing] their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of the service to make free and informed decisions"[81]. Article 25 provides three specific examples: (1) "Giving more prominence to certain choices when asking the recipient […] for a decision", (2) "Repeatedly requesting that they recipient […] make a choice where that choice has already been made", and (3) "Making the procedure for

[79] EP and Council of the EU, Reg. 2022/1925, September 14, 2022, on contestable and fair markets in the digital sector (Digital Markets Act, known as the DMA).

[80] BEUC, 2022, p. 12.

[81] DSA, Article 25(1).

terminating a service more difficult than subscribing to it"[82]. Notably, the words "dark patterns" do not appear in the Article itself. Nevertheless, the accompanying Recital 67 clarifies that the prohibition includes them. The recital defines dark patterns as the "structure(s), design(s) or functionalities" of "online interfaces of online platforms [that] materially distort or impair, either in purpose or effect, the ability of recipients to make autonomous and informed choices or decisions. [They] can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them"[83].

The prohibition on dark patterns extends only to online platforms; defined as intermediary service providers who host user-generated information and disseminate it to the public at the user's request[84]. Public dissemination occurs when such information is made available to a potentially unlimited number of people, regardless of how many actually access it[85]. The prohibition applies regardless of the platform's place of establishment, so long as it provides services to users in the EU[86]. Since February 2024, the DSA has applied to all online intermediaries offering their services (goods, content, or services) in the European market: internet service providers (ISPs), cloud computing services, online platforms like marketplaces, app stores, social networks, content-sharing platforms, travel and accommodation platforms, very large online platforms,

---

[82] DSA, Article 25.

[83] DSA, Recital 67. Recital 67 also lists several specific examples of prohibited patterns: “Giving more prominence to certain choices” ; “Repeatedly requesting a recipient of the service to make a choice where such a choice has already been made” ; “Making the procedure of cancelling a service significantly more cumbersome than signing up to it” ; “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” ; and “Default settings that are very difficult to change”.

[84] DSA, Article 3(i) DSA ; DSA, Recital 13.

[85] DSA, Recital 14.

[86] DSA, Article 2(1).

and very large search engines used by more than 45 million Europeans per month. This category specifically targets the GAFAM companies (Google, Apple, Facebook, Amazon, and Microsoft), even if they are not directly named. Nevertheless, to avoid imposing disproportionate obligations, the prohibition does not apply to micro or small enterprises[87], nor to intermediaries who only publicly disseminate user content as an ancillary feature[88]. At the other end are "recipients of the service", who may be all sorts of users, including both consumers and business users[89].

The DSA prohibits design choices or user interface experiences on online platforms that manipulate or deceive users in a way that impairs their autonomy. In establishing autonomy as its benchmark, Article 25 targets practices that nudge a recipient into a choice contrary to their preferences; or impair the exercise of autonomy such that the user is unable to define their own preferences[90]. Intermediaries may impair user choices through "the structure, design or functionalities of an online interface"[91], and hence Article 25 forbids the manipulative "design, organisation and operation" of such interfaces. Another element of the prohibited conduct is that its effect of deceiving or manipulating recipients must be "material". The DSA itself does not clarify if the effect must be actual or if a potential effect may suffice. Nor does it clarify what materiality is. A related question is what the recipient standard should be when evaluating whether a practice is deceptive: how savvy must the recipient be? Should the UCPD's "average consumer" standard be used? Finally, Article 25(2) clarifies that the DSA prohibition

[87] DSA, Article 19.

[88] DSA, Article 3(i).

[89] DSA, Article 3(b) ; DSA, Recital 2.

[90] DSA, Article 25.

[91] DSA, Recital 67.

shall not apply to practices covered by the GDPR and the UCPD[92]. This begs the question of what scope is left for the DSA prohibition.

On October 4, 2024, the European Commission published its findings following the Digital Fairness Check[93], which aims to evaluate whether current EU consumer protection rules are adequate to address challenges posed by recent technological developments and increased tracking of online behavior. The report mentions, among other issues, (i) dark patterns, e.g., interface designs that can unfairly influence consumer decisions; (ii) addictive design, e.g., functionalities that abusively encourage consumers to continue using a service, such as gambling-like features in video games; (iii) personalized targeting features that take advantage of consumers' vulnerabilities; (iv) features that make it excessively difficult for consumers to cancel digital subscriptions. This substantial report highlights online practices likely to be central to the upcoming European Commission regulation proposal aimed at revitalizing European online consumer protection rules: the Digital Fairness Act[94]. The Digital Fairness Act proposal will likely aim to harmonize the applicable rules (including the UCPD, DSA, DMA, Data Act…) to create a level playing field within the EU internal market.

[AI Regulation] The European legislator has gone even further than its foreign counterparts by addressing the potential evolution of dark patterns at the dawn of the "artificial intelligence (AI) era". AI could, in fact, make these strategies more effective by

---

[92] DSA, Article 25(2).

[93] European Commission, 2024.

[94] The Digital Fairness Act (DFA) is a legislative proposal by the European Commission. Commissioner Michael McGrath will be responsible for this legislation under Ursula von der Leyen's second Commission. The legislation will tackle dark patterns and influencer marketing. See European Commission (Michael McGrath - Mission letter), 2024.

enabling a better understanding of user behavior, allowing for precise targeting of specific segments based on observed and inferred characteristics. As noted by the Stigler Center, the use of dark patterns is likely to be amplified through the use of artificial intelligence: "Dark patterns are often used to direct users towards outcomes that involve greater data collection and processing. Additionally, the proliferation of data-driven computational methods allows firms to identify vulnerabilities of users and to target specific users with these vulnerabilities"[95]. In other words, AI could enable the personalization of manipulations. To achieve this, AI systems may use subliminal components, such as auditory, visual, or video stimuli that are beyond human perception, or other manipulative or deceptive techniques that subvert or compromise a person's autonomy, decision-making, or free will, to the point where they are not consciously aware of these techniques, or if they are aware, they may still be deceived or unable to resist or control them. Some AI systems may exploit vulnerabilities of an individual or specific groups of people due to their age, disability as defined by Directive (EU) 2019/882 of the European Parliament and Council[96], or their particular social or economic situation, making them more vulnerable to exploitation, such as people living in extreme poverty or ethnic or religious minorities. For all these reasons, the first global AI regulation, the European AI Act, prohibits the marketing, commissioning, or use of any AI system that employs behavioral manipulation techniques[97].

[95] Stigler Center, 2019, p. 238.

[96] EP and Council of the EU, Directive 2019/882, April 17, 2019, on accessibility requirements for products and services (Text with relevance to the EEA).

[97] EP and Council of the EU, Reg. 2024/1689, June 13, 2024, establishing harmonized rules on artificial intelligence (Artificial Intelligence legislation, known as the AI Act).

✚ **Regulation 2024/1689, June 13, 2024, laying down harmonized rules on Artificial Intelligence (AI Act)**

The AI Act is the first comprehensive AI regulation established by a major regulatory body. It categorizes AI applications into three risk levels: unacceptable, high risk, and low risk. Recital 29 notes that "he placing on the market, the putting into service or the use of certain AI systems with the objective to or the effect of materially distorting human behaviour, whereby significant harms, in particular having sufficiently important adverse impacts on physical, psychological health or financial interests are likely to occur, are particularly dangerous and should therefore be prohibited"[98]. Hence, under Article 5(1)(a), the AI Act bans "the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm"[99]. Recital 29 clarifies that the prohibition of these AI practices complements the provisions of Directive 2005/29/EC of the European Parliament and Council on unfair commercial practices causing economic or financial harm to consumers. These practices are prohibited in all circumstances, whether through AI systems or otherwise.

[98] IA Act, Recital 29.

[99] IA Act, Article 5 (1)(a).

2.2 In the United States of America

Despite substantial scholarship on dark patterns, U.S. federal law and courts have not proactively used the term when issuing decisions regulating manipulative user interfaces. U.S. laws and courts have relied on a fragmented and generic legal framework to address dark patterns. Instead, courts have generally applied existing doctrines when dealing with manipulative contractual designs, such as classic contract law and the Children's Online Privacy Protection Act (COPPA). However, U.S. policymakers have recently shown growing interest in specifically regulating dark patterns. States such as California, Colorado, and Connecticut now explicitly prohibit dark patterns, but only those aimed at obtaining consumer consent for the processing of their personal data.

2.2.1 Federal legislation

[General legislation, Contract Law & Common Law Principles] In the absence of specific law, American contract law and the general principles of Common Law indirectly prohibit dark patterns. These could notably be challenged under the doctrine of "unconscionability". This doctrine is a contractual defense, typically invoked in cases where a combination of unfair contract terms and unbalanced negotiations are present. "Unconscionability" was introduced into American contract law by the adoption of English law in the former colonies. The concept gained momentum with the 1954 promulgation of the Uniform Commercial Code (UCC) and its section 2-302 (U.C.C. §2-302). The merging of equitable law and Common Law, along with the codification of this merger, led to a general

recognition of "unconscionability" in contract law. Neither the UCC nor the 1981 Restatement[100] provides a precise definition of "unconscionability". However, the official commentary to UCC section 2-302 suggests that the goal is to prevent oppression and unfair surprises. This concept has been interpreted to include both procedural and substantive elements. Procedural unconscionability concerns deficiencies in the way the contract was formed, such as the exploitation of disparities in the status and sophistication of the parties, misleading appearances or language in the contract, and questionable negotiation practices. Substantive unconscionability refers to the contract terms themselves, often characterized by an excessive imbalance in favor of one party or a particularly shocking clause[101]. The most famous case dealing with unconscionability is probably *Williams v. Walker-Thomas Furniture Company*, decided in 1965[102]. In this case, Judge J. Skelly Wright ruled that the case should return to trial to assess more facts, but clarified that a contract may be invalidated if it was established through unconscionable methods. He stated that contracts should not be enforced if there is unconscionability at the time of formation. Unconscionability exists when one party lacks meaningful choice due to significant bargaining power inequality, and the contract terms disproportionately benefit the other party. The fairness of the process by which the contract was signed is also important, particularly if the terms were unclear or hidden. In cases where a party with little bargaining power signs an unreasonable contract without full knowledge, courts should reconsider enforcing such terms. These criteria allow for the legal challenge of contractual dark patterns, especially when they are used to exploit consumer

---

[100] Restatement (Second) of Contracts §208, 1981.

[101] See e. g. Henningsen v. Bloomfield Motors, Inc., 32 N.J. 358, 161 A.2d 69 (N.J. 1960). In this case, the plaintiff, Mr. Henningsen, had purchased a car that turned out to be defective, leading to an accident and injuries to his wife. The sales contract included a clause limiting the manufacturer's liability, but the New Jersey Supreme Court found this clause to be unfair and against public policy. The court determined that ordinary consumers, like the Henningsens, did not have the ability to negotiate or fully understand such clauses in an adhesion contract (a standardized contract offered by a powerful party to a weaker party without any opportunity for negotiation).

[102] Williams v. Walker-Thomas Furniture Co., 350 F.2d 445 (D.C. Cir. 1965). See also Williams v. Walker-Thomas Furniture Co., 198 A.2d 914 (D.C. 1964).

vulnerability or lack of information, thus compromising the fairness and integrity of the contractual process.

[Specific legislation, Consumer & Data Protection Laws] However, similar to Europe, U.S. law that could be considered "special" also contains provisions for protecting against manipulative practices in the commercial context. For example, though acting indirectly, the Federal Trade Commission Act (also called "FTC Act") of 1914 (as further amended)[103], and more specifically Section 5(a) of the FTC Act prohibits "[…] unfair or deceptive acts or practices in or affecting commerce […]"[104]. The law, which applies broadly to commercial activities and practices likely to affect consumers, therefore regulates dark patterns. It is usefully complemented by the Children's Online Privacy Protection Act (COPPA) of 1998[105], which "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet"[106].

Federal Trade Commission Act (FTC Act) of 1914, 15 U.S.C. §45(a)

Section 5(a) of the FTC Act, codified at 15 U.S.C. §45(a), gives the Federal Trade Commission (FTC) the power to prohibit and regulate unfair or deceptive commercial practices. As previously cited, 15 U.S.C. §45(a)(1) makes it illegal, in addition to unfair methods of competition, to engage in deceptive acts or practices in commerce[107].

---

[103] Federal Trade Commission Act, September 26, 1914 codified at 15 U.S. Code (U.S.C.), Ch. 2, Subchapter 1, §§41-58.

[104] 15 U.S.C. §45(a)(1).

[105] Children's Online Privacy Protection Act, October 21, 1998 (16 Code of Federal Regulations (C.F.R.), §312) codified at 15 U.S.C., Ch. 91, §§6501-6508.

[106] 15 U.S.C. §6502.

[107] 15 U.S.C. §45(a)(1).

"Deceptive" practices are defined in the Commission's Policy Statement on Deception[108] as involving a material representation, omission, or practice that is likely to mislead a consumer acting reasonably under the circumstances. According to the Commission's Policy Statement on Unfairness[109], referencing 15 U.S.C. §45(n), an act or practice is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"[110]. 15 U.S.C. §45(a)(2) gives the FTC the authority to investigate and take action against companies engaged in such practices[111].

Under the Federal Trade Commission Act, the Federal Trade Commission combats the use of unfair or deceptive practices that affect commerce in interstate trade[112]. In this role, the FTC has filed actions against several companies for using dark patterns, even if some cases do not specifically use this term[113]. Furthermore, after holding a workshop on dark patterns in April 2021[114], the FTC also released a policy enforcement statement specifically on dark patterns in October 2021[115]. In this statement, the FTC clearly indicated that it would intensify actions against dark patterns that trick consumers into subscribing to services or trap them when they

---

[108] FTC, Policy Statement on Deception, 1983.

[109] FTC, Policy Statement on Unfairness, 1980.

[110] 15 U.S.C. §45(n).

[111] 15 U.S.C. §45(a)(2).

[112] Some relevant cases are FTC v. Lending Club, 3:18-cv-02454 (N.D. Cal. 2020), FTC v. ABC mouse, 2:20-cv07996 (C.D. Cal. 2020), FTC v. Vonage Case 3:22-cv-06435 (D.N.J. 2022), FTC v. Vizio 2:17-cv-00758 (D.N.J. 2017) etc.

[113] See e. g. Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 1-45, U.S. v. Epic Games, Inc., 5:22-CV-00518-BO (E.D.N.C. 2023).

[114] Bringing Dark Patterns to Light: an FTC workshop, April 29, 2021. Following the workshop organized by the FTC, a report on dark patterns titled *"Bringing Dark Patterns to Light"* was published on September 15, 2022. In this report, the FTC identifies four widespread and problematic categories of dark patterns and announces targeted legal actions: -Deception of consumers and disguised advertising; - Making cancellation difficult; - Burying key terms (under layers of jargon) and hidden costs; - Tricking consumers into providing more personal data. See FTC, Staff Report "Bringing Dark Patterns to Light", September 2022.

[115] FTC, Enforcement Policy Statement Regarding Negative Option Marketing, October 28, 2021.

attempt to cancel ("trick or trap dark patterns"). U.S. companies face penalties if they fail to provide "clear, upfront information when obtaining consumer consent at sign-up" and if they do not make cancellations easy. Privacy and data protection bills also expressly mention dark patterns as practices to be prohibited. However, no federal law has yet been passed, likely due to political pressures. The first significant federal legislative proposal to combat dark patterns was the Deceptive Experiences To Online Users Reduction (DETOUR) Act, introduced in April 2019 by U.S. Senators Deb Fischer and Mark Warner. The bill aims to restrict the use of dark patterns by large online companies. It was reintroduced in July 2023[116]. Despite its reintroduction, there have been no significant updates on the progress of this legislation. In 2022, the American Data Privacy and Protection Act (ADPPA) was introduced to regulate how organizations handle consumer data, prohibiting manipulative user interfaces that undermine autonomy[117]. Despite bipartisan support, the bill wasn't brought to a vote. Finally, in April 2024, a new draft, the American Privacy Right Act (APRA)[118], was proposed. APRA aims to create comprehensive data privacy laws, banning dark patterns that obscure consent or impair user rights[119]. It prioritizes protecting minors and imposes stricter rules on large data holders, with the FTC overseeing enforcement. Efforts to introduce specific federal legislation have been abundant, yet good intentions alone seem insufficient. Interestingly, federal action primarily operates through the FTC, an independent agency responsible for

---

[116] Bill for Federal Law: Deceptive Experiences To Online Users Reduction Act, July 27, 2023, S. 2708, 118th Cong. This bill seeks to prohibit large online operators to "design, modify, or manipulate a user interface on an online service with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision making, or choice to obtain consent or user data", §3(a)(1).

[117] Bill for Federal Law: American Data Privacy and Protection Act, June 21, 2022, H.R. 8152, 117th Cong. More specifically, the law prohibited obtaining consent through "the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to provide such consent or any covered data" §2(1)(D)(ii).

[118] Bill for Federal Law: American Privacy Right Act, June 25, 2024, H.R. 8818, 118th Cong. §101(16) ; §107(a).

[119] Ibid.

enforcing consumer protection laws, whereas at the state level, privacy protection laws take the lead.

2.2.2 States legislation

[In California] The California Consumer Privacy Act (CCPA) of 2018, amended by the California Privacy Rights Act (CPRA)[120], provides the first definition of dark patterns in U.S. law: "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".

+ California Consumer Privacy Act (CCPA) of 2018 & California Privacy Rights Act (CPRA) of 2020

In the CCPA, dark patterns were not explicitly included in the text. However, the California Attorney General's regulations referenced vague instructions to "promote consumer awareness"[121], "ensure that the notices and information…are provided in a manner that may be easily understood by the average consumer"[122], and "minimize the administrative burden on consumers"[123]. These regulations include an unnamed definition of dark patterns: "a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt out"[124]. The

---

[120] California Consumer Privacy Act, June 28, 2018 amended by California Privacy Rights Act, November 3, 2020 codified at California Civil Code (Cal. Civ. Code) §§1798.100-1798.199. The accompanying regulations are found at 11 CCR §§7000 & seq. 11 California Code of Regulations (Cal. Code Regs.) §§7000-7304.

[121] Cal. Civ. Code §1798.185(1)(4)(3); note, all citations to the CCPA may no longer be valid due to the CPRA superseding them.

[122] Cal. Civ. Code §1798.185(1)(6).

[123] Cal. Civ. Code §1798.185(1)(7).

[124] 11 Cal. Code Regs. §7026(h).

regulations provided examples such as, "a request to opt-out shall not require more steps than to opt-in"[125], "a business shall not use confusing language"[126], and "the business shall not require the consumer to search or scroll through the text of a privacy policy"[127] among others[128]. The CPRA, on the other hand, explicitly mentions dark patterns three times. First, it defines dark patterns as "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"[129]. Notably, this definition focuses on the effects of the interface, not the designer's intent. The proposed regulations provide examples[130], such as using a larger "yes" button for accepting cookies than the "no" button[131]. Second, the law states that "agreement obtained through the use of dark patterns does not constitute consent"[132]. The CPRA explicitly prohibits obtaining consent for data processing through dark patterns; consent cannot be coerced or manipulated. The CCPA was also amended to prohibit dark patterns during the opt-out process[133]. Finally, the law gives the CPPA authority to promulgate rules regarding opting-out of the sale or share of personal information with the instruction that any link "does not make use of any dark patterns"[134]. The proposed CPRA regulations offer a broader exploration of dark patterns than the CCPA. They

---

[125] 11 Cal. Code Regs. §7026(h)(1).

[126] 11 Cal. Code Regs. §7026(h)(2).

[127] 11 Cal. Code Regs. §7026(h)(5).

[128] The other examples listed in 11 Cal. Code Regs. §7026(h), are other inconveniences to deter consumers from enforcing their rights, which are also dark patterns.

[129] Cal. Civ. Code §1798.140(l); all citations to CPRA are current California law.

[130] 11 Cal. Code Regs. §7004(a)(2)-(5) for examples.

[131] 11 Cal. Code Regs. §7004(a)(2)(D)

[132] Cal. Civ. Code §1798.140(h).

[133] 11 Cal. Code Regs. §7013(e)(5); §7015(c)(2); §7020(d); §7025(c)(3); §7026(b); §7027(c); §7028(b) and (c).

[134] Cal. Civ. Code §1798.185(20)(C)(iii).

outline numerous principles businesses must follow to process requests or obtain consumers' consent[135]. Both the CCPA and CPRA impose fines of $2,500 per violation, or $7,500 if the violation is intentional. Although there are few examples of prosecutions, it is expected that California will be more aggressive in enforcing these regulations than other jurisdictions.

Specific regulations have also been adopted in California to protect vulnerable users, particularly minors. Modeled after the United Kingdom's Age-Appropriate Design Code (UK AADC)[136], the California Age-Appropriate Design Code (CAADC) [137]requires internet companies to assess potential risks for young users on their platforms and to implement, by default, the strongest protective settings for those users. This complements the CPRA by focusing specifically on dark patterns targeting minors. The California law extends beyond the federal Children's Online Privacy Protection Act (COPPA) by covering more online services and expanding protections to all individuals under 18. Effective since July 1, 2024[138], the Code defines dark patterns and prohibits businesses from using them to encourage children to provide unnecessary personal information, give up privacy protections, or take actions detrimental to their physical or mental well-being[139].

[In several other States] It is important to note that California is not the only U.S. state regulating dark patterns. Other states have also implemented direct regulations on this

[135] 11 Cal. Code Regs. §7004(a)

[136] United Kingdom's Age Appropriate Design Code, January 27, 2020. It took effect September 2, 2020 with a one-year grace period before the beginning of enforcement.

[137] California Age-Appropriate Design Code Act, September 16, 2022 codified at Cal. Civ. Code §§1798.99.28-1798.99.40.

[138] Ibid, Cal. Civ. Code §1798.99.31. (d).

[139] Cal. Civ. Code §1798.99.31. (b)(7).

issue. Alongside the CPRA, the Colorado Privacy Act (CPA)[140] explicitly mentions dark patterns, prohibiting their use when obtaining consent[141]. The CPA defines dark patterns as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice"[142]. This Act went into effect on July 1, 2023. Similarly, Connecticut takes a limited view of these techniques. The Connecticut Data Privacy Act (CTDPA)[143] defines dark patterns[144] and states that agreements obtained through their use do not constitute valid consent[145]. This Act, which also took effect on July 1, 2023, is limited to consent manipulation interfaces. The Maryland Legislature approved the Maryland Online Data Privacy Act of 2024 (MODPA) on April 6, 2024, which is expected to be signed into law by Governor Wes Moore and take effect on October 1, 2025. The Act explicitly mentions dark patterns and excludes agreements obtained through their use from the scope of "consent". Similarly, the Nebraska Data Privacy Act, approved in April 2024, outlines specific thresholds, includes language for universal opt-out mechanisms, and prohibits the use of dark patterns to obtain consent from data subjects. This Act defines dark patterns as user interfaces designed or manipulated to substantially subvert or impair user autonomy, decision-making, or choice. To conclude, the CPRA, CPA, and other state laws seem to focus primarily on the use of dark patterns for collecting personal data. This excludes other types of dark patterns that do not involve personal data obligations but are nonetheless manipulative and deceptive (e.g., "sneak into basket", price comparison prevention, nagging,

---

[140] Colorado Privacy Act, July 7, 2021, codified at Colorado Revisited Statutes (Colo. Rec. Stat.) §6-1-1301, & seq. The CPA is a part of the State of Colorado's Consumer Protection Act.

[141] Colo. Rev. Stat. §6-1-1303 (5)(c)

[142] Colo. Rev. Stat. §6-1-1303 (9)

[143] Connecticut Data Privacy Act, May 10, 2022 codified at Connecticut General Statutes (Conn. Gen. Stat.) §42-515 & seq.

[144] Conn. Gen. Stat. §42-515 (14), "Dark pattern means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

[145] Conn. Gen. Stat. §42-515 (7)

scarcity). While defining dark patterns is crucial for regulation, the regulations implemented in U.S. states appear to adopt a narrow understanding of manipulation techniques and dark patterns. Unless judges and regulatory authorities interpret these prohibitions broadly based on the existing definitions, federal law currently appears to offer more protection. However, compared to European law, U.S. law seems more fragmented, dispersing into numerous special laws without providing a comprehensive regulatory response to manipulation and deception by design. This is especially evident when analyzing state laws that focus on prohibiting privacy-related dark patterns.

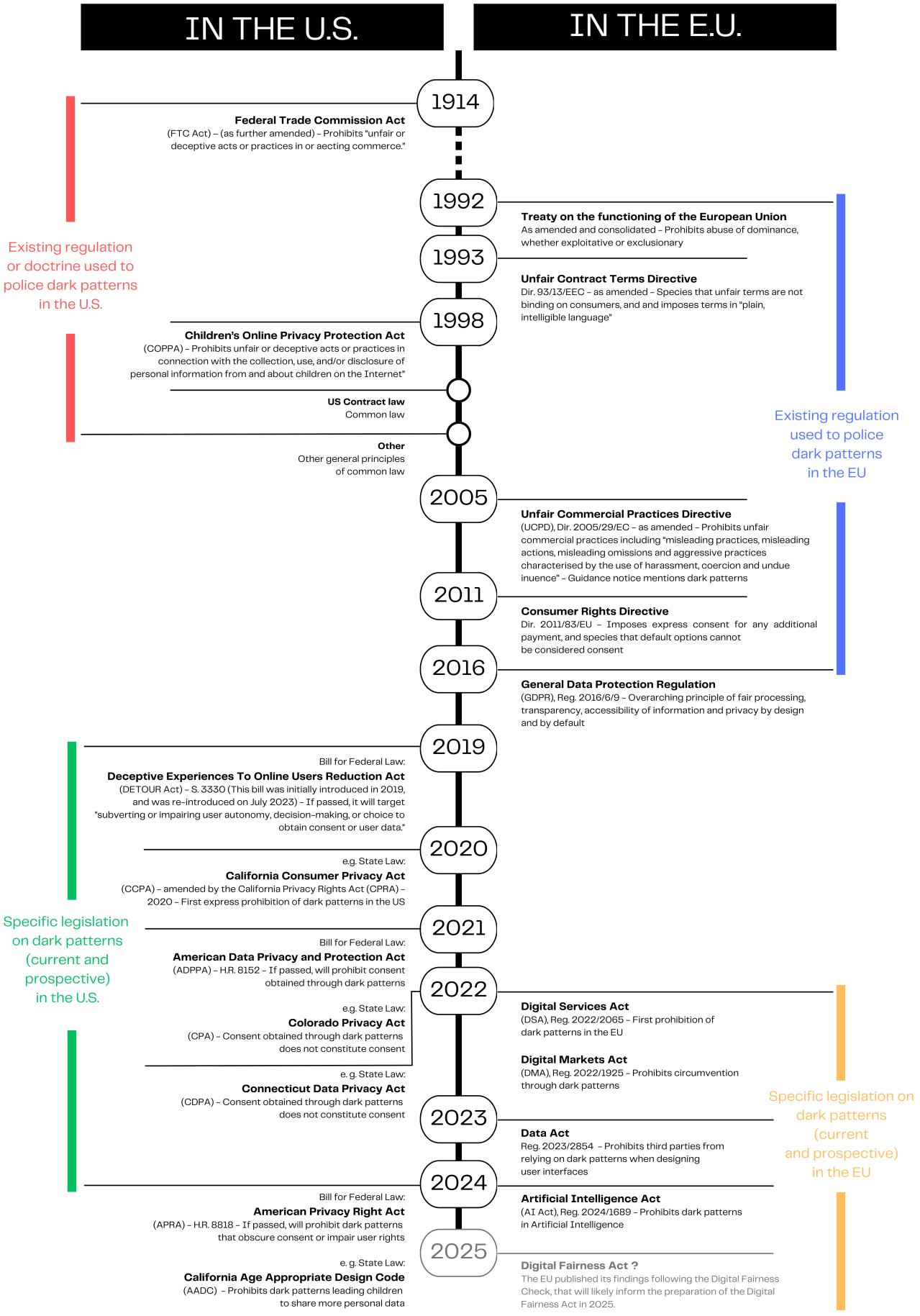

Fig. 5. Evolution of legislation policing dark patterns (U.S./E.U.)

CONCLUSION

[Limits of the Digital World] Our digital interactions are heavily influenced by the use of dark patterns. These deceptive and manipulative design techniques are highly effective, offering short-term economic incentives and immediate advantages to their creators. However, dark patterns distort the proper functioning of the market. In the long run, their use harms consumers, who are forced to sacrifice their privacy by accepting obscure privacy policies or entering into contracts they had no intention of agreeing to. By weakening market competition, dark patterns can lead to a global market imbalance, where consumer interests are compromised in favor of deceptive and manipulative business strategies. Beyond the market, dark patterns also disrupt the "social contract". Our social contract, which is based on values like trust, solidarity, and transparency, is endangered. The subtle manipulation of decision-making environments in the digital space cannot be justified, as platforms often claim, by the promise of a high-quality customer experience. We no longer purchase—we are extorted. We no longer consent—we are violated. We no longer share—we are spied upon. The philosophy of dark patterns is "do as I tell you, not as you think". Merchants, and sometimes even non-merchants, have industrialized manipulation processes, just as they once industrialized production processes.

[Limits of the Law] Of course, the legislator is neither deaf nor blind. The law has attempted in several ways to better regulate these practices. However, legislators are limited in their understanding of observable practices, regulators in their enforcement capabilities, and the law in its clarity for the affected parties. While the law deserves credit for naming and

banning manipulative practices, it often restricts its scope of intervention in numerous texts. This is particularly the case in the United States, where dark patterns are often reduced to consent manipulation techniques for data collection in many states. Yet, dark patterns have multiple faces, take different forms, and serve various functions. Sometimes they appear as static interfaces, other times as interactive ones, or even as complex experiences. Unfortunately, regulators have adopted an overly simplified view of the concept and its problems. While the text of the law may be interpreted broadly—one can assume that the European legislator had this in mind when choosing to establish a broad, vague, and non-restrictive definition—the lack of precision raises concerns. Legislators do not offer evaluation criteria for determining what is fair and what is not. An analysis of the texts thus highlights certain gaps or weaknesses resulting from a lack of clarity in the terms used and the scope of application. This raises questions about the effectiveness and efficiency of these new European regulatory provisions.

[Design for Law] This emerging "dark patterns law" also contains a more systemic limitation—a legislative design issue. As usual, legislators focus on the substance of the law but pay little attention to its form, i.e., its design. This is not unique to digital law but is observed in other regulatory domains as well. For example, contract law does not give sufficient attention to the design of contracts, just as administrative law does not sufficiently address the form of administrative acts. The "dark patterns law" will be limited because the legal areas it intersects with (data protection, consumer law, etc.) are not precise enough about their form in the digital space. If privacy policies are incomprehensible and terms of sale are endless, it becomes easy, quick, and even pleasant to accept them with a single click.

This partly explains why the adage "ignorance of the law is no excuse" remains a fantasy, while "no one is expected to understand the law" is a reality. By focusing solely on the substance of the law—its "informativity"—and neglecting its form, or "communicativeness", the legislator has left considerable leeway for digital interface designers to adapt the communication of legal information and thereby guide legal decisions according to their economic interests. The responses provided by regulators tend to focus exclusively on legal or technical aspects, which is a mistake. While both aspects are essential, they are insufficient to address the exposed challenges. They do not sufficiently take into account the interaction space between the user and the machine. It is precisely within this interaction space that pressure is exerted on the user. The design choices made by an app's creator inevitably influence the user. Yet, paradoxically, design seems to struggle to find its place among the intervention tools of regulators. The common field of intervention between traditional regulation and design thus remains to be defined—a task that will be the subject of the next study.

BIBLIOGRAPHY

Article

Acquisti, A. Adjerid, I. Balebako, R. Brandimarte, L. Cranor, L. Komanduri, S. Leon, P. Sadeh, N. Schaub, F. Sleeper, M. Wang, Y. & Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. ACM Comput. Surv. 50(3), pp. 1-41.

Akerlof, G. A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics, 84(3), pp. 488-500.

Coase, R. H. (1937). The nature of the firm, Economica, 4(16), pp. 386-405.

Dahlman, C. J. (1979). The Problem of Externality. The Journal of Law & Economics. 22 (1), pp. 141-62.

Dwork, C. McSherry, F. Nissim, K. & Smith, A. (2016). Calibrating Noise to Sensitivity. Private Data Analysis Journal of Privacy and Confidentiality. 7(3), pp. 1-20.

Dwork, C. & Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science. 9(3-4), pp. 211-407.

Faure, M. G. & Luth, H. A. (2011). Behavioural Economics in Unfair Contract Terms Cautions and Considerations. Journal of Consumer Policy. 34(3), pp. 337-358.

Hosseini, H. (2003). The Arrival of Behavioral Economics: From Michigan, or the Carnegie School in the 1950s and the Early 1960s. Journal of Socio-Economics. 32(4), pp. 391-409.

Jarovsky, L. (2022). Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness. SSRN. pp. 1-51.

Kahneman, D. & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. Econometrica. 47(2), pp. 263-291.

Luguri, J. & Strahilevitz, L. J. (2021). Shining a light on dark patterns. Journal of Legal Analysis. 13(1), pp. 43-109.

March, J. G. Simon, H. A. (1958), Organizations, New York: Wiley.

McDonald, A. M., Cranor, L. F. (2008). The cost of reading privacy policies. A Journal of Law and Policy for the Information Society. 4(3), pp. 543-565.

Maier, M., & Harr, R. (2020). Dark design patterns : An end-user perspective. Human Technology, 16(2), pp. 170-199.

Miller, K., Sahni, N.S., Strulov-Shlain, A. (2022). Sophisticated Consumers with Inertia: Long-Term Implications from a Large-Scale Field Experiment. Becker Friedman Institute - Working Paper, pp. 1-67.

Morozovaite, V. (2023). The future of anticompetitive self-preferencing: analysis of hypernudging by voice assistants under article 102 TFEU (2023) European Competition Journal, 19(3).

Potel Saville, M. (2022). Dark Patterns: l'étau législatif se resserre (enfin?) sur les interfaces manipulatrices ou trompeuses. Revue Pratique de la Prospective et de l'Innovation. 6(2), pp. 41-47.

Simon, H. A. (1959). Theories of Decision-Making in Economics and Behavioral Science. American Economic Review. 49(3), pp. 253-283.

Smythe, D. W. (1950). Television and Its Educational Implications. Elementary English, 27(Jan), pp. 41-52.

Sunstein, C. & Thaler, R. (2003). Libertarian Paternalism is Not an Oxymoron. University of Chicago Law Review. 70(4), pp. 1159-1202.

Sunstein, C. (2014). Choosing not to choose. Duke Law Journal. 64(1), pp. 1-52.

Susser, D. Roessler, B. & Nissenbaum, H. F. (2019). Online Manipulation: Hidden Influences in a Digital World. Georgetown Law Technology Review. 4(1), pp. 1-45.

Thaler, R. & Sunstein, C. (2003). Libertarian Paternalism. American Economic Review. 93(2), pp. 175-179.

Wagner, G. (2010). Mandatory Contract Law: Functions and Principles in Light of the Proposal for a Directive on consumer rights. Erasmus Law Review. 3(1), pp. 47-71.

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the "privacy paradox". Current opinion in psychology, 31, pp. 105-109.

Zachrisson, J. & Boks, C. (2012). Exploring behavioral psychology to support design for sustainable behavior research. Journal of Design Research. 10(1/2), pp. 50-66.

Book

Bacache-Beauvallet, M. & Bourreau, M. (2022). Économie des plateformes. Paris: La Découverte.

Bacqué, M-H. & Biewener, C. (2013). L'Empowerment, une pratique d'émancipation. Paris: La Découverte.

Bar-Gill, O. (2012). Seduction by Contract: Law, Economics and Psychology in Consumer Markets. Oxford: Oxford University Press.

Citton, Y. (2014). L'économie de l'attention : Nouvel horizon du capitalisme ?. Paris: La Découverte.

Kahneman, D. (2011). Thinking, Fast and Slow. Londres: Penguin Books.

Mansell, R. (2012). Imagining the Internet: Communication, Innovation and Governance. Oxford: Oxford University Press.

Pareto, V. (1963). Manuel d'Économie Politique. Paris: Pichon.

Rochelandet, F. (2010). Économie des données personnelles et de la vie privée. Paris: La Découverte.

Simon, H. A. (1947). Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization. New York: Macmillan.

Shapiro, C. & Varian, H. R. (1999). Information Rules. A Strategic Guide to the Network Economy, Boston: Harvard Business School Press.

Thaler, R. H. & Sunstein, C. R. (2008). Nudge: Improving decisions about health, wealth and happiness. New haven: Yale University Press.

Verhelst, E. W. (2012). Recht Doen aan Privacyverklaringen: een Juridische Analyse van Privacyverklaringen op Internet. Alphen aan den Rijn: Wolters Kluwer.

Vial, S. (2015). Le Design. Paris: Presses Universitaires de France.

Zuboff, Sh. (2020). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Zulma.

Zuiderveen Borgesius, F. (2015). Improving Privacy Protection in the Area of Behavioural Targeting. Alphen aan den Rijn: Wolters Kluwer.

Book Chapter

Acquisti, A. & Grossklags, J. (2007). What Can Behavioral Economics Teach Us about Privacy. In A. Acquisti & al. (Eds), Digital Privacy: Theory, Technologies and Practices (pp. 363-377). New York: Auerbach Publications.

Graef, I. (2023). The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law? (2023). In A. Ramsi & al. (Eds), Toward an

Inframarginal Revolution: Markets as Wealth Distributors. Cambridge: Cambridge University Press.

Schäfer, H-B., & Leyens, P. (2010). Judicial Control of Standard Terms and European Private Law. In P. Larouche, & F. Chirico (Eds.), Economic Analysis of the DCFR: The Work of the Economic Impact Group within the CoPECL Network of Excellence (pp. 99-121). Munich: Sellier European Law Publishers.

Simon, H.A. (1971). Designing organizations for an information-rich world. In M. Greenberger (Ed.), Computers, Communications and the Public Interest (pp. 37-72). Baltimore: John Hopkins Press.

Communication published in proceedings

Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. In Proceedings of the 5th ACM Conference on Electronic Commerce (pp. 21–29). New York: Association for Computing Machinery Library.

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021). "I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous !" – Dark Patterns from the End-User Perspective. In Designing Interactive Systems Conference 2021 (pp. 763-776). New York: Association for Computing Machinery Library.

Di Geronimo, L. Braz, L. Fregnan, E. Palomba, F. & Bacchelli, A. (2020). UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In CHI 2020 - Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-14). New York: Association for Computing Machinery Library.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In CHI 2018 - Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-14). New York: Association for Computing Machinery Library.

Gray, C., Santos, C. & Bielova, N. (2023). Towards a Preliminary Ontology of Dark Patterns Knowledge. In CHI 2023 - Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems). (pp. 1-9). New York: Association for Computing Machinery Library.

Gunawan J., Pradeep A., Choffnes D., Hartzog W. & Wilson Ch. (2021). A Comparative Study of Dark Patterns Across Mobile and Web Modalities. In Proceedings of the ACM 2021

Conference on Computer-Supported Cooperative Work and Social Computing (pp. 1-29). New York: Association for Computing Machinery Library.

Jensen, C. & Potts, C. (2004). Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In CHI 2004 - Proceedings of the 2004 CHI Conference on Human Factors in Computing Systems (pp. 471-478). New York: Association for Computing Machinery Library.

Mathur, A., Mayer, J. & Kshirsagar, M. (2021). What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In CHI 2021 - Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems: Making Waves, Combining Strengths (pp. 1-27). New York: Association for Computing Machinery Library.

Potel-Saville, M. & Da Rocha Francois, M. (2023). From Dark Patterns to Fair Patterns? Usable Taxonomy to Contribute Solving the Issue with Countermeasures - Proceedings of the 2023 Annual Privacy Forum.

Voigt, C. Schlögl, S. & Groth, A. (2021). Dark Patterns in Online Shopping: Of Sneaky Tricks, Perceived Annoyance and Respective Brand Trust. In CHI 2021 - Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 143-155). New York: Association for Computing Machinery Library.

Report

Authority for Consumers and Markets (ACM). (2022). Guidelines on Consumer Protection in Online Environments: The Limits of Online Persuasion. Netherlands Authority for Consumers and Markets.

European Consumer Organisation (BEUC). (2022). "Deceptive Interfaces" and the EU Consumer Acquis. Recommendations for Better Enforcement and Reform.

European Commission. (2021). Guidelines on the Interpretation and Application of Directive 2005/29/EC of the European Parliament and of the Council on Unfair Commercial Practices by Businesses in the Internal Market.

European Commission. (2022). European Declaration on Digital Rights and Principles for the Digital Decade.

European Commission. (2024). Digital fairness – fitness check on EU consumer law.

European Commission. (2024). Michael McGrath - Mission letter.

European Data Protection Board (EDPB). (2023). Guidelines 03/2022 adopted on 14 February 2023 on Deceptive Design Patterns in Social Media Platforms.

UK Competition and Markets Authority. (2022). Online choice architecture: how digital design can harm competition and consumers.

European Union Commission. (2022). Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation.

Federal Trade Commission (FTC). (1983). Policy Statement on Deception.

Federal Trade Commission (FTC). (1980). Policy Statement on Unfairness.

Federal Trade Commission (FTC). (2021). Enforcement Policy Statement Regarding Negative Option Marketing.

Federal Trade Commission (FTC). (2022). Staff Report "Bringing Dark Patterns to the Light ".

Information Commissioner Office (ICO). Competition and Markets Authority (CMA) and Digital Regulation Cooperation Forum (DRCF). (2023). Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information.

Laboratoire d'Innovation Numérique de la Commission Nationale Informatique et Liberté (LINC, CNIL). (2019). La forme des choix. Cahiers IP Innovation & Prospective. 6.

Organisation for Economic Cooperation and Development (OECD). (2022). Dark Commercial Patterns, OECD Digital Economy Working Papers. 336.

SciencesPo - Chaire Digital, Governance and Sovereignty. (2023). Policy Brief. "Comment l'Union européenne devrait-elle réglementer les interfaces truquées ? ".

Stigler Center. (2019). Report of the Committee for the Study of Digital Platforms. Chicago: University of Chicago.

Press article/blog

Brignull H. Deceptive Design.

Cario, E. (2018, 16 août). Jacques Testart: "Le transhumanisme est une idéologie infantile", Libération.

Hagan, M. Why Law Needs Design. TTC Labs.

Sinders, C. (2021). Designing against dark patterns. German Marshall Fund of the United States.

Zappi, S. (2013, 7 février). L’ "empowerment", nouvel horizon de la politique de la ville, Le Monde.