Dark Patterns in Personal Data Collection: Definition, Taxonomy, and Lawfulness

Luiza Jarovsky

I. Introduction

Alice heard it is important to protect her privacy, so she opens her favorite social network and looks up the settings, to check that everything is ok. She has some difficulty with how to proceed, as some of the configurations are under "settings and privacy," others under "visibility," others under "sign in & security," and yet others under "data privacy." Moreover, after clicking each link there are additional texts with information, drop-down menus with multiple links, links that redirect her to external URLs and buttons whose meaning are unclear. It all seems too complicated and she gives up, feeling certain that her interests are not correctly reflected in the configurations.

Bob starts reading a newspaper article on a trending political topic, and when he wants to scroll down, the screen is blocked, and a banner appears asking him to create an account. The signup button says "Signup and never miss out on the next hot topic!" He feels that it is better to sign up and be up to date with political news than to be lazy. The signup screen asks for his name, email, telephone, and home address, and also requests that he checks boxes referring to his personal interests (so that the articles can be specially tailored for him) and to accept to receive marketing offers by email and SMS. He would rather not receive any marketing offers, but when he unselects

these options, a banner appears stating that "some of the website's functionalities might not work well," so he selects them back, feeling there is no other option.

Charlie recently started using a new social app focused on funny videos. He considers himself a shy person, so the possibility of recording short clips using filters, music, and subtitles seems to be a good opportunity to surprise his closest friends. He takes care not to add anyone as a friend there so that he can start recording 'in secret' and practice with the app tools before he shares with anyone. It is easy and immediate to record, so he spends hours creating funny dances animated by pop music. When he goes to sleep, strangely, his phone beeps non-stop. It turns out that the default setting of this app is to share all videos publicly and to allow others to download them. An influencer with a large following reposted one of Charlie's videos using an offensive hashtag and tagged him, and now there are hundreds of people adding their own offensive comments on his videos and re-uploading edited versions. Charlie became a meme and feels helpless.

Danah works online all day and is really annoyed with the number of banners requesting consent for cookie collection. The two options that are usually offered are "accept all" and "more information." She does not really know what cookies are, so once she clicked the "more information" and dozens of green switches with unknown names appeared, and these companies seemingly were collecting her data. It would take too much time to turn off all the switches, and she cannot see very well; therefore, since then, she just clicks "accept all" every time. She heard that the parliament in her

country enacted a Data Protection Law, so she feels confident that nothing bad will happen. Recently, she started receiving various email offers from a business she had never heard of. She has also been receiving SMS and calls from sales representatives; it is usually hard to distinguish what is legitimate and what is not, as the offers tend to be suitable for her. Last week a privacy organization informed Danah that her credit card information was among the data leaked from a company she never heard about, so she should cancel her card. She feels helpless with the internet and wishes she could just live like in the old times.

The cases above are adaptations of real situations commonly experienced online. All of them contain one or more *dark patterns in privacy* (DPPs), and, unfortunately, they are common in today's online landscape, even among services run by publicly traded global companies.

In this article, I argue that DPPs represent a challenge to global privacy laws, including the European Union (EU) data protection framework and the General Data Protection Regulation (GDPR),[1] which is the main jurisdictional focus of this article.

DPPs involve the exploitation of cognitive biases and the deployment of exploitative techniques to manipulate data subjects through the interface design of apps and websites. I contend that despite the apparent absence of legal tools to deal with DPPs, the current EU framework can be adapted and amended to identify and curb them, especially through the fairness principle.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).

I am especially motivated by the complexity of the study of dark patterns in the privacy context, which involves interdisciplinary analysis of design, human-computer interaction (HCI), computer science, cognitive psychology, behavioral economics, ethics, and law. Law has traditionally refrained from closely regulating design,[2] given the supposed risk of hindering technological innovation or being too rigid to adapt to the varied and rapidly changing set of business practices. DPPs, however, have the potential to create ruptures in the web of protections currently afforded to data subjects and lower the already volatile amount of trust that is awarded to service providers. Therefore, this article aims to integrate these various fields of knowledge through the discussion of cognitive biases that underlie many DPPs, their manifestation within technological environments, the rationale behind their deployment, and their legal meaning.

Dark patterns do not target exclusively personal data; they consist of a broader phenomenon and can affect other areas such as one's finances, emotions, attention, and so on.

The term *dark patterns* was first coined in 2010 by Harry Brignull,[3] who launched a website called *darkpatterns.org*.[4] Brignull defined dark patterns as "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something."[5]

---

[2] For the challenges of regulating design, see WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).

[3] Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design.

[4] Today renamed to http://deceptive.design.

[5] *Id.*

In recent years, awareness around the topic has grown, and the HCI, computer science, and legal literature offer various descriptions of dark patterns,[6] as well as legal frameworks such as the California Consumer Privacy Act,[7] the EU's Digital Services Act (DSA).[8]

When discussing the essence of DPPs, it is important to raise the topic of nudges. Juxtaposing DPPs and nudges may clarify some of the boundaries and help understand how dark patterns differ from other practices.

A nudge, a term coined by Richard Thaler and Cass Sunstein, is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a

---

[6] Such as: "instances where designers use their knowledge of human behavior (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest" – see Colin Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin Toombs, *The Dark (Patterns) Side of UX Design*, CHI 2018, 1 (2018). "Intent on the part of the designer to deliberately sacrifice the user experience in an attempt to achieve the designer's goals ahead of those of the user" – see Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, INTERNATIONAL WORLD WIDE WEB CONFERENCE COMMITTEE 271, 1 (2010). Interfaces whose goal is "to exploit cognitive vulnerabilities to guide users towards targeted choices" see Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?* 72 ALA. L.R 1, 3 (2020). "Interface designs that try to guide end-users into desired behaviour through malicious interaction flows" – see Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, Lalana Kagal, *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, CHI '20, 3 (2020). "User interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make" - see Arunesh Mathur, et al, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites,* PROCEEDINGS OF THE ACM HUMAN-COMPUTER INTERACTION 3 CSCW, ARTICLE 81, 2 (2019). "Features of interface design crafted to trick users into doing things that they might not want to do, but which benefit the business in question" and "deliberately misleading users through exploitative nudging" – see Forbrukerrådet, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage us From Exercising our Rights to Privacy*, at 7 (2018), https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf.

[7] See California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(l). "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."

[8] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

nudge. Banning junk food does not."[9] Designers, therefore, can manipulate interface design elements to steer individuals in a certain direction, nudging them.

Despite this author's negative stand on the deployment of nudges without openness and transparency on the agenda of the choice architect,[10] in this article, not all nudges will be considered dark patterns.[11] To be considered a dark pattern, the design must be manipulative *and* have as an objective goal to make the data subject worse off according to the observed criteria. The observed criterion, in the present article, is privacy, or whether the data subject is worse off in terms of privacy protection. A design that is manipulative but does not necessarily lead the data subject to a negative outcome can be said to be morally problematic,[12] as the designer is trying to encourage the user to take a different course of action through the exploitation of cognitive biases. However, despite the wrongful means, the end goal might be beneficial, deriving from a background of ethical design,[13] as it happens with some nudges. For example, interface designs that nudge people to eat fewer calories or protect their privacy will not be considered dark

---

[9] RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH AND HAPPINESS, 6 (2009).

[10] For this author, nudges are problematic, as they rely on cognitive biases to steer people in a desired direction. A frequent example of nudges is the deployment of defaults that make people save money or donate organs after death. These examples might seem inoffensive and actually beneficial to the individual or to society. However, autonomy and human dignity are also important values and there might be situations in which both individual and society would benefit more from a well thought or personalized choice according to the concerned individual's values, beliefs and rights. Moreover, the argument that the individual can still choose other alternatives when nudges are present is weak, as if nudges are effective, they leave little or no space for deeper reflection and consideration of values and ideas that are different than those advanced by the choice architect.

[11] Manipulative design is one that "does not sufficiently engage or appeal to their capacity for reflection and deliberation." Cass Sunstein, *Fifty Shades of Manipulation*, 1 J. MARK. BEHAV. 213, 218 (2016).

[12] On the deontological argument against manipulation, see Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQ. L. 157, 175 (2019).

[13] "Excellent designs would be those where the designer takes social responsibility and the ethical measures of a designed product into account. If we want to entrust a livable world for our children in the future, then the ethical design criterion should be adapted and implemented as one of the basic principles of design requirements." See Ahmet Atak & Aydın Şık, *Designer's Ethical Responsibility and Ethical Design*, 7 U. J. MECH. ENG. 255, 262 (2019).

patterns,[14] even if they eventually cause the affected person to behave against their own preferences and wishes.[15] Therefore, manipulation without the objective negative goal will not be considered a dark pattern.

The article proceeds as follows: Section II proposes a definition for DPPs, taking into consideration the relevant elements for the present analysis as well as the distinction made above between dark patterns and nudges. Section III brings the general premises and the conceptions of privacy that influence how I approach DPPs. Section IV presents and discusses the cognitive biases involved in DPPs, showing how they affect data subjects, especially in the privacy context. Section V proposes a taxonomy for DPPs, offering various examples and a visual representation of each category. Section VI discusses DPPs' legal status, evaluating the possibilities within the EU legal framework that could legitimize or outlaw them, taking into consideration existing rules and principles. Section VII compares two decision-making paradigms that can be applied to data subjects: *Homo economicus* and *Homo manipulable*, arguing in favor of the latter, which reflects behaviors and traits observed in real life. Lastly, Section VIII concludes by pointing to the avenues to legally outlaw and prevent DPPs.

II. Definition of DPP

[14] Importantly, these interface designs can, nevertheless, cause harm, as they assume what is good or bad without consulting the affected individuals or considering their personal preferences. Mccrudden and King commented on the possible dangers of nudges: "(i)f we emphasize the tendency to 'counteract' biases, then we see that some forms of nudging seem to rely on psychological insights to try to ensure 'good' results. They 'attempt to harness cognitive irrationalities in aid of desired social policy outcomes." See Christopher Mccrudden & Jeff King, *The Dark Side of Nudging: The Ethics, Political Economy, and Law of Libertarian Paternalism,* RESEARCH PAPER 485, U. MIC. PUB. L. 67, 105 (2015).

[15] In the case, for example, in which a person is trying to gain weight or being purposefully privacy negligent.

Given the focus of the present article, which aims at understanding the current legal standing of DPPs and proposing changes in the current framework that would improve the protection offered to data subjects, I propose the following working definition for DPPs:

> *A dark pattern in privacy is an interface design choice that manipulates the data subject's decision-making process in a way detrimental to their privacy and beneficial to the service provider.*

I explain each of its elements:

"interface design choice": a DPP materializes when the data subject interacts with the interface design of a product or service. The service can be provided through a browser, an app, or any other type of technology, and if the data subject can interact with an interface designed by the service provider, DPP can exist. The terminology "design choices" is also important, as it highlights that behind the seemingly value-neutral appearance of a service, there are choices involved and professionals with expertise in designing interfaces that can be effective for business but also harmful to the data subjects' interests,[16] such as a DPP.

"that manipulate the data subjects' decision-making process: to manipulate someone can be defined as "intentionally and covertly influencing their decision-making, by targeting and

[16] For a deeper analysis on how design can be deployed to positively impact privacy, see Richmond Wong & Deirdre Mulligan, *Bringing Design to the Privacy Table, Broadening "Design" in "Privacy by Design" through the Lens of HCI*, CHI 2019 (2019).

exploiting their decision-making vulnerabilities."[17] DPPs are manipulative because they rely on cognitive biases to steer the data subject's decision-making process in the desired direction.

"in a way detrimental to their privacy": to be considered a dark pattern, the data subject's decision has to be detrimental to their privacy in the sense that the data subject is pushed to share more or more sensitive data, as I further develop in Section III. Accordingly, a nudge or a manipulation that aims at protecting the data subject's privacy or that helps them understand more about privacy, better navigate settings, share less data, or share data with fewer people is not a dark pattern. DPPs differ in which cognitive biases they exploit, but all of them exacerbate the information and power asymmetry between data subjects and data controllers. When a designer has an agenda to amplify data collection and surreptitiously twists interface elements to steer the data subject in a certain direction, the designer deprives the data subject of a fair decision-making process regarding their privacy.[18]

"and beneficial to the service provider": this is one of the outcomes of dark patterns. By keeping the data subject uninformed regarding privacy choices and their outcomes, turning data subjects away from scrutinizing how their data is used, promoting unnecessary data sharing, fostering a culture of unrestrained and unconscious disclosure of personal data, and so on, controllers and their partners are beneficiaries of DPPs.

---

[17] Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y. REV. 1, 4 (2019).

[18] The harm to data subject can also be framed in terms of autonomy loss, see Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1 (2019).

The proposed definition differs from other existing approaches to dark patterns as it breaks down the specific *modus operandi* of dark patterns in privacy, and will facilitate the discussion in the next Sections. It highlights the parties involved (data subjects, service providers), the type of manipulation (place: interface design; how: altering the decision-making process), and the outcome (detrimental to privacy, beneficial to the service provider).

In the next section, I clarify the premises and the privacy theories that inform the present analysis.

III. Premises and Privacy Theories

Despite making us feel frustrated, surprised, trapped, ashamed, powerless, and so on, it is necessary to explain why and how DPPs are objectively harmful to privacy.

An important premise that needs to be clarified is that calling something a DPP involves a moral judgment. The working definition, as set in the previous Section, requires a designer steering us in a certain direction that makes us worse off. But how can we objectively assess what is a good or a bad outcome? Some cases are easy, as legal principles and rules make it clear what is the legally expected way to act. For example, a design technique that tricks someone into spending more money than they intended leads to a bad outcome, as it is a form of manipulation. On the other hand, a design that calls attention to the safety issues of a certain product is good, as it is one of the principles of worldwide consumer protection and tort laws.[19]

[19] See, e.g., Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

However, some cases are not so easy, as there are legal, cultural, and religious differences that result in different perceptions of what is good or bad, right, or wrong. For example, what about a design that makes people work more? Or a design that makes people spend more time online interacting with other people? Or a design that promotes the desire to be thin? There are numerous grey areas, as it is a discussion of human values, not an exact science.

Any honest analysis of dark patterns must be transparent regarding the values at stake. The present article explores dark patterns in the field of privacy. Therefore, I need to be clear about what conception of privacy I am referring to and what will be considered a negative impact on privacy.

This article relies on two main definitions of privacy. The first is Alan Westin's, which states that privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[20] Westin's definition reflects a model of control in which the individual has agency over how their personal information is shared.[21] It implies that personal data can only be amplified or processed to the extent lawfully consented or legally authorized. This model correctly acknowledges the data subject's autonomy and freedom, expecting them to be the manager of their choices regarding their personal data. It is also aligned with Fair Information Practice Principles (FIPPs)[22] and data

---

[20] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

[21] According to Birnhack, "privacy as control is best understood as a concretization of the overarching idea of dignity, applied to personal issues." Michael Birnhack, *A Process-Based Approach to Informational Privacy and the Case of Big Medical Data*, 20 THEORETICAL INQ. L. 257, 263 (2019).

[22] According to Schwarz, "fair information practices are the building blocks of modern information privacy law. They are centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight." Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999).

protection laws that rely on data subjects' consent as one of the possibilities for lawful processing.[23]

Despite correctly emphasizing user autonomy, there are numerous shortcomings of consent in privacy, which were studied by legal and HCI scholars[24] and categorized by this author.[25] Given that we are specifically dealing with situations in which user agency is suppressed or inflected – and the data subject cannot properly choose – an additional definition is necessary, one that does not rely on the data subject's control and recognizes any negative interference in the decision-making process as a harm to privacy.

Following this line of thought, the other approach I will utilize is Ruth Gavison's, who defined the interest in privacy as "related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention."[26] Despite being presented in the 1980s – the pre-internet era – Gavison's focus on access precisely captures the idea that we might want some people or entities not to have any access to us. It allows a conception of privacy as a state in which we are shielded from external entities attempting – which sometimes rely on exploitative techniques as it happens with DPP – to collect more personal data.

---

[23] I.e. Article 6(1)(a) of the GDPR establishes that "processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes."

[24] See Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013); Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 649 (2011); Lorrie Faith Cranor, *Necessary but Not Sufficient, Standards Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273 (2012); Lizzie Coles-Kemp & Elahe Kani-Zabihi, *On-line Privacy and Consent: A Dialogue not a Monologue*, PROCEEDINGS OF THE 2010 WORKSHOP ON NEW SECURITY PARADIGMS - NSPW '10, 95 (2010).

[25] See Luiza Jarovsky, *Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs)*, 4 EUR. DATA PROTECTION L. 447 (2018) (proposing a classification of the shortcomings of consent).

[26] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980).

I wish to emphasize that this article's approach is not context-dependent, meaning that it does not matter if we are dealing with medical, intimate, or social media data.[27] The threshold for negatively impacting privacy is the attempt to abuse the data subject's decision-making capacity to access their personal data[28] in whatever context it happens. Therefore, I assume that any manipulative technique that supports, by action or inaction, additional sharing of personal data or the disruption of the decision-making process regarding privacy can be considered negative – a harm to privacy.

Another important premise is that this article deals only with manipulative practices that occur within design interfaces. There are, however, other types of manipulative techniques that can negatively impact privacy online. Some of these techniques operate, for example, through unfair privacy policies, artificial intelligence (AI) algorithms, and product policies and functionalities.

In the next Section, I turn to the topic of cognitive biases affecting DPP, first explaining their general manifestation and then how they occur in the privacy context.

IV. Cognitive Biases affecting DPP

An important part of the study of DPP is understanding the cognitive biases they exploit. A cognitive bias is a "systematic (that is, nonrandom and, thus, predictable) deviation from

---

[27] Here, I do not examine the nuances reflected in contextual informational norms. The appropriateness of information flows is important, and I intend to explore it in a subsequent analysis. In this article, I focus on limiting the access that controllers have to data subjects' personal data. For a more detailed approach on the value of contextual integrity for privacy law, see HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

[28] Through the exploitation of cognitive biases and implementation of DPP.

rationality in judgment or decision-making."[29] Cognitive biases can also be understood in terms of the process that leads to them and the effects generated by them.[30] The process is a heuristic process,[31] and the result is the bias.

Cognitive biases were originally discussed by cognitive psychologists such as Amos Tversky and Daniel Kahneman,[32] who identified that "people rely on a limited number of heuristic principles which reduce the complex tasks of assessing probabilities and predicting values to simpler judgmental operations. In general, these heuristics are quite useful, but sometimes they lead to severe and systematic errors."[33]

Cognitive biases are inherent human traits and can be empirically demonstrated.[34] If privacy law wants to protect real humans (*i.e.*, not distorted or outdated theoretical models of human rationality), it must correctly acknowledge cognitive biases and their consequences for the decision-making capacity of data subjects.

Based on Tversky and Kahneman's approach to heuristics and mental shortcuts and considering decision-making contexts in which data subjects must make a privacy-relevant choice,

---

[29] Fernando Blanco, *Cognitive Bias*, *in* ENCYCLOPEDIA OF ANIMAL COGNITION AND BEHAVIOR, 1 (Jennifer Vonk & Todd Shackelford eds., 2017).

[30] Gaëlle Lortal, Philippe Capet & Alain Bertone, *Ontology Building for Cognitive Bias Assessment in Intelligence*, IEEE INTERNATIONAL INTER-DISCIPLINARY CONFERENCE ON COGNITIVE METHODS IN SITUATION AWARENESS AND DECISION SUPPORT 237, 237-238 (2014).

[31] "A strategy that ignores part of the information, with the goal of making decisions more quickly, frugally, and/or accurately than more complex methods." Gerd Gigerenzer & Wolfgang Gaissmaier, *Heuristic Decision Making,* 62 ANNUAL REV. PSY. 451, 454 (2011).

[32] A discussion was conducted by Paul Slovic, Ellen Peters, Melissa Finucane, Donald MacGregor, *Affect, Risk, and Decision Making*, 24 HEALTH PSY. 35 (2005).

[33] Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124, 1124 (1974). There are also opposite views of the cognitive biases theory, which consider them to be advantages, such as Gerd Gigerenzer & Henry Brighton, *Why Biased Minds Make Better Inferences,* 1 TOP. COGN. SCI. 107 (2009).

[34] For a deeper view on cognitive biases and their empirical demonstration, see DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011) and DAN ARIELY, PREDICTABLY IRRATIONAL (2010).

such as when facing a cookie banner or navigating privacy settings, I gathered a non-exhaustive list of cognitive biases commonly exploited by DPP.

The cognitive biases listed in this section illustrate the diversified nature of manipulative practices in the context of privacy decision-making and reflect a practical manifestation of Tversky and Kahneman's concept of heuristics in the field of privacy.

Their presentation in relation to the heuristic principle—or mental shortcut—they reflect, and the explanation of how they impact individuals in the privacy context, are relevant for the comprehension of the aspects of human decision-making that must be taken into consideration by data protection law. The analysis also helps expand the existing body of knowledge on cognitive biases and heuristics by contextualizing them from a data protection perspective.

1. Anchoring and Adjustment Heuristic: Anchoring Bias

"Systematic influence of initially presented numerical values on subsequent judgments of uncertain quantities, even when presented numbers are obviously arbitrary and therefore unambiguously irrelevant."[35] This bias has been discussed extensively and demonstrated in behavioral psychology, including studies from Tversky and Kahneman[36] and popular culture books.[37] An offline example would be the case of a restaurant owner who adds dishes that are very expensive to the first pages of a restaurant menu; the client will then be anchored by higher values and will consider the remaining dishes' values to be lower and advantageous, even if they are expensive when compared to those of similar restaurants.

---

[35] Predrag Teovanović, *Individual Differences in Anchoring Effect: Evidence for the Role of Insufficient Adjustment,* 15 EUR. J. PSYCHOL. 8, 8 (2019).

[36] Tversky & Kahneman, *supra* note 29.

[37] See ARIELY, *supra* note 139.

This bias has been exploited in the privacy context, for example, when presenting privacy options to the data subject. In a privacy menu, the pool of values from which the data subject can choose is typically arbitrary, with the designer deciding what are the broadest-sharing options and the least-sharing options. Relying on the anchoring bias, the designer can choose a first option that is privacy-negligent and additional options that are only mildly protective. The data subject is 'anchored' by the first option and induced to perceive the additional options as being privacy protective.

2. Social Proof Heuristic: Bandwagon Effect

"The case where an individual will demand more (less) of a commodity at a given price because some or all other individuals in the market also demand more (less) of the commodity."[38] This bias has similar roots to "group-think" and "herd effect," where the behavior of the individual is modified by the behavior of the collective.[39] It can be observed in multiple contexts, such as when rating the attractiveness of female faces[40] or in Asch-type social conformity experiments.[41]

Over the past decade, its occurrence in social networks and its impact on privacy have been particularly acknowledged. For example, it was observed that "whether and how much one used Facebook was unequivocally coupled with its diffusion within the global, local, and communal

---

[38] Harvey Leibenstein*, Bandwagon, Snob, and Veblen Effects in the Theory of Consumers' Demand*, 64 Q.J. ECON. 183, 190 (1950).

[39] Lindsey Levitan & Brad Verhulst*, Conformity in Groups: The Effects of Others' Views on Expressed Attitudes and Attitude Change*, 38 POLITICAL BEHAV. 277 (2016).

[40] Vasily Klucharev Kaisa Hytönen Mark Rijpkema, Ale Smidts & Guillén Fernández, *Reinforcement Learning Signal Predicts Social Conformity*, 61 NEURON 140 (2009).

[41] Rod Bond, *Group Size and Conformity*, 8 GROUP PROCESS INTERGROUP RELAT. 331 (2005). "The original Asch study on conformity is recognized as a classical experiment in social psychology. The experiment demonstrated the tendency of participants to conform when under the pressure of a unanimous majority." Knud Larsen, *The Asch Conformity Experiment: Replication and Transhistorical Comparisons*, 5 J. SOC. BEHAV. PERS. 163, 163 (1990).

contexts."[42] We can observe the bandwagon effect anecdotally on a daily basis in social networks, where the quick popularity of memes and trending topics shows the immense interconnectedness within these networks. In the privacy context, the consequence of the bandwagon effect is that if negligent privacy attitudes are trending (*i.e.*, people share photos, videos, and personal data without restraint), they will be reproduced among other users of the network as well.[43]

3. Contrast Perception Heuristic: Contrast Effect

The contrast effect to which I am referring here involves visual aspects: exploring the relationship between two objects (or two texts) to reduce readability or to generate a desired impression in the observer/reader. An example is that "several studies indicate that increased contrast between the text and background results in increased readability."[44] Therefore if the designer wishes that a certain text is not noticed or well read, the designer should apply low contrast in the color scheme. A well-known example were the techniques used by search engines in the past to blur the difference between sponsored and organic results.[45] This effect is also commonly observed when the designer selects low contrast schemes for privacy-protective options in an attempt to steer data subjects' attention off and reduce the probability that they will choose restrictive options.

---

[42] Wayne Fu, Jaelen Teo, Seraphina Seng, *The Bandwagon Effect on Participation in and Use of a Social Networking Site*, 17 FIRST MONDAY (2012).

[43] It is important to notice that there will always be culture and social norms. This bias, on the other hand, specifically highlights the constant correlation of the individual attribution of value to the collective attribution of value, without a dedicated thought process or contextual considerations.

[44] Robert Moore, Claire Stammerjohan & Robin Coulter, *Banner Advertiser- Web site Context Congruity and Color Effects on Attention and Attitudes*, 34 J. ADVERTISING 71, 73 (2005).

[45] In 2013, the Federal Trade Commission (FTC) sent letters to search engine companies asking for more differentiation between paid and natural results, in order to avoid consumer deception and violation of Section 5 of the FTC Act. Similar letters had been sent in 2002, with the same argument. FTC, *FTC Consumer Protection Staff Updates Agency's Guidance to Search Engine Industry on the Need to Distinguish Between Advertisements and Search Results* (Jun. 25, 2013), https://www.ftc.gov/news-events/press-releases/2013/06/ftc-consumer-protection-staff-updates-agencys-guidance-search.

4. Status Quo Heuristic: Default Effect

The default effect is the observation that the default option "is chosen more often than expected if it were not labeled the default."[46] Various explanations for the "stickiness" of defaults exist, including the absence of effort needed and the appearance of an implied endorsement by the service provider. The default effect bias has been observed in multiple contexts, among the most famous being organ donation and retirement savings plans.[47]

Defaults are prevalent in the privacy field as well, and it has been shown that individuals will most commonly stick to the default privacy option instead of taking time to think and choose a more suitable alternative.[48] It is known that designers have been benefiting from this bias for a long time by defining privacy-invasive defaults.[49] More recently, with the rise of Privacy by Design (PbD) and Data Protection by Design and by Default and with the requirement for explicit consent,[50] defaults that are patently detrimental to the data subject are not so frequently seen anymore, but it is worth noticing that there is no express ban on defaults, therefore leaving room for companies to imply that certain data is necessary or essential for the performance of the service, with no external accountability.[51]

---

[46] Isaac Dinner, Eric Johnson, Daniel Goldstein, Kaiya Liu, *Partitioning Default Effects: Why People Choose Not to Choose*, 17 J. EXP. PSY.-APPL. 332, 335 (2011).

[47] For a broader review, see Lauren Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155 (2013).

[48] *Id.*

[49] See Matthew Keys, *A Brief History of Facebook's Ever-changing Privacy Settings*, MEDIUM.COM (Mar. 21, 2018), https://medium.com/@matthewkeys/a-brief-history-of-facebooks-ever-changing-privacy-settings-8167dadd3bd0. On a more positive side, for an analysis on the optimization of access control defaults in online social networks, see Ron Hirschprung, Eran Toch, Hadas Schwartz-Chassidim, Tamir Mendel & Oded Maimon, *Analyzing and Optimizing Access Control Choice Architectures in Online Social Networks*, 8 ACM TRANS. INTELL. SYST. TECHNOL., Article 57 (May 2017).

[50] GDPR, Article 4(11). The topics of PbD and DPbDD will be dealt in more detail on Section VII.2 *infra*.

[51] Unless it is a paid service or any specific business model that does not rely on advertising or data.

5. Framing Heuristic: Framing Effect

"The 'framing effect' is observed when a decision maker's risk tolerance (as implied by their choices) is dependent upon how a set of options is described."[52] More specifically, "people appear to exhibit a general tendency to be risk-seeking when confronted with negatively framed problems and risk-averse when presented with positively framed problems."[53] The framing effect has been observed in multiple contexts,[54] and studies have been conducted to find ways to reduce its impact.[55] An example of its manifestation is the performance comparison of advertising a yogurt as 1% fat or 99% fat-free. "The percentage-fat-free format led to stronger endorsements of healthiness than the percentage-fat format,"[56] showing the impact of the framing effect on the perception of healthiness.

In the privacy context, the designer can frame choices and options to elicit a less privacy-protecting option. For example, when asking if the data subject wishes to begin using a face identification service, the designer can highlight the novelty, sophistication, and surprises that the technology can bring, leaving problematic privacy issues as a side comment or something that does not deserve the same level of detail.

---

[52] Cleotilde Gonzalez, Jason Dana, Hideya Koshino & Marcel Just, *The Framing Effect and Risky Decisions: Examining Cognitive Functions with fMRI*, 26 J. ECON. PSY. 2 (2005).

[53] *Id.*

[54] See Sammy Almashat, Brian Ayotte, Barry Edelstein & Jeniffer Margrett, *Framing Effect Debiasing in Medical Decision Making*, 71 PATIENT EDUC. COUNS. 102 (2008). Antony Sanford, Nicolas Fay, Andrew Stewart, Linda Moxey, *Perspective in Statements of Quantity, with Implications for Consumer Psychology*, 13 PSY. SCI. 130 (2002).

[55] See Mathieu Cassotti et al, *Positive Emotional Context Eliminates the Framing Effect in Decision-Making*, 12 EMOTION 926 (2012).

[56] Antony Sanford et al., *supra* note 159, at 132.

6. Present Bias Heuristic: Hyperbolic Discounting

"People's choices are often intertemporally inconsistent, for example, in the sense that people prefer a larger, later consumption bundle over a smaller, sooner one as long as both are sufficiently distant in time, but change their preference to the smaller, sooner bundle as both draw near."[57] In less technical terms, an individual would value $50 now more than $100 in a month.

In a privacy-related context, this means that an individual often prefers to use a service immediately, even if it involves risks or possible long-term privacy impacts, instead of not using the service now and preserving their privacy long-term. Privacy scholars have acknowledged this bias in studies about privacy policies and how people prefer to simply click "I accept" and be submitted to aggressive terms so that they can immediately enjoy the service.[58]

*

As seen above, cognitive biases are diverse,[59] reflecting the various tools and techniques used by designers to manipulate the data subject's decision-making capacities. These biases have been extensively described in cognitive psychology and behavioral economics literature, but their integration with data protection law and the specific acknowledgment of their potential to support privacy harm are still missing.

---

[57] Till Grüne-Yanoff, *Models of Temporal Discounting 1937–2000: An Interdisciplinary Exchange between Economics and Psychology*, 28 SCIENCE IN CONTEXT 675, 677 (2015).

[58] See Alessandro Acquisti & Jens Grossklags, *Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior*, UC BERKELEY 2ND ANNUAL WORKSHOP ON ECONOMICS AND INFORMATION SECURITY (2003). Alessandro Acquisti, Leslie John, George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUDIES 249 (2013).

[59] Kahneman & Ariely's books cited *supra* at note 139.

The next Section advances the discussion by proposing a taxonomy for DPPs based on the different ways in which design choices can negatively impact the data subject's privacy-related decision-making process.

V. Taxonomy

Scholars and national organizations have proposed taxonomies for dark patterns in general, including those affecting money, emotions, attention, and data. Among the national organizations are the Norwegian Consumer Council (Forbrukerrådet)[60] and the French National Commission on Informatics and Liberty (CNIL).[61] Among the scholars are Hartzog,[62] Calo,[63] Frisch,[64] Brignull,[65] Conti & Sobiesk,[66] Nouwens et al.,[67] Bösch et al.,[68] Gray et al.,[69] Mathur et al.,[70] and Zagal et al.[71]

---

[60] Forbrukerrådet, *supra* note 110.

[61] Laboratoire d'Innovation Numérique de la CNIL, *IP Report: Shaping Choices in the Digital World, From dark patterns to data protection: the influence of UX/UI design on user empowerment* (2019), https://www.cnil.fr/sites/cnil/files/2023-06/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[62] HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 106.

[63] Ryan Calo, *Digital Market Manipulation*, 27 GEO. WASH. L. REV. 995 (2013).

[64] Lothar Frisch, *Privacy Dark Patterns in Identity Management*, *in* OPEN IDENTITY SUMMIT 2017: PROCEEDINGS 93 (Lothar Fritsch, Heiko Roßnagel, Detlef Hühnlein, eds., 2017).

[65] Brignull, *supra* note 107.

[66] *Supra* note 110.

[67] *Supra* note 110.

[68] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, Stefan Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns,* PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 237 (2016).

[69] Colin Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin Toombs, *The Dark (Patterns) Side of UX Design*, CHI 2018 (2018).

[70] *Supra* note 110.

[71] José Zagal, Staffan Björk, Chris Lewis, *Dark Patterns in the Design of Games*, FOUNDATIONS OF DIGITAL GAMES CONFERENCE (2013), http://www.fdg2013.org/program/papers/paper06_zagal_etal.pdf.

Among all the above mentioned, only four (Forbrukerrådet, CNIL, Nouwens et al., and Zagal et al.) have proposed some form of classification system for dark patterns in the privacy field, but only the two national organizations (Forbrukerrådet and CNIL) offered a more overarching taxonomy for dark patterns in privacy.

Forbrukerrådet's categorization focuses on five forms of DPP: "default settings," "ease," "framing," "rewards and punishment," and "forced action and timing." Despite the richness of the examples offered and the useful comparison between Facebook, Google, and Microsoft's systems, this taxonomy does not fully portray the spectrum of DPP as reflected in the categories that will be presented *infra* and does not show how cognitive biases can be used to form dark patterns or how the data subject is impacted.

CNIL, the French data protection authority, developed a non-exhaustive typology including a broader spectrum of DPP, offering a useful and deep overview of the topic. In CNIL's approach, the categories of dark patterns in privacy are "enjoy," "seduce," "lure," "complicate," and "ban." Each of them can either "push the individual to accept sharing more than what is strictly necessary," "influence consent," "create friction on data protection actions," or "divert the individual." Despite offering no less than 18 examples that have certainly influenced this author to think more broadly about dark patterns, the logic behind their classification does not match the analysis of the present article, which focuses on the ways in which decision-making was affected.

Given the unsuitability of existing taxonomies for the present article's analysis, I propose a new classification, the premises and methodology of which I explain now.

The first step in elaborating the taxonomy was finding academic articles and other public sources with categories and examples of dark patterns in order to understand which of them were specifically targeting personal data. The public repositories I found were the website

deceptive.design the Twitter account connected to the same website (@darkpatterns) - where the public can share their examples of dark patterns - and the Tumblr account https://confirmshaming.tumblr.com. The academic papers I used as sources of examples of dark patterns were those cited above, especially the reports by Forbrukerrådet and CNIL, which dealt with privacy-related dark patterns.

After gathering several examples of DPP, my task was to develop categories and groups that matched them and helped me advance the present analysis, understanding how exactly they affect the decision-making capacities of data subjects. For this purpose, I needed a deeper legal approach regarding decision-making and the factors that would make a certain decision to be deemed invalid or unlawful.

In private law, the integrity of the decision-making process is analyzed through civil law and the study of consent and consent defects. Given that the jurisdictional focus of the present article is the EU, and the fact that the EU does not have a single civil code, I resorted to the Principles of European Contract Law (PECL).[72]

The PECL provided a unified view of the EU approach to contractual principles and rules, including those pertaining to the topic of consent and consent defects. Among all the causes of invalidity of contracts,[73] those that are related to the decision-making process of one of the contracting parties are a) mistake, b) fraud, c) threats,[74] and d) excessive benefit or unfair advantage.[75] In the presence of one of these situations, the damaged party may avoid the contract, according to the additional rules of the same Chapter within the PECL.

---

[72] Principles of European Contract Law, https://www.trans-lex.org/400200.

[73] PECL, Chapter 4.

[74] PECL, Article4:108.

[75] PECL, Article4:109.

The four categories above represent a central pillar in the study of the validity of consent within the realm of contract law.[76] Here, I am importing these ideas to the sphere of data protection law, and investigating how designers can negatively affect the data subject's decision-making process, including the validity of the obtained decision/consent.

When transposed to data protection law, I adapted the four contractual categories so that they would match typical privacy decision-making situations, especially regarding a) the way the data subject is negatively impacted; and b) the action performed by the data controller.

First, the idea of "threat" was translated as "pressure."[77] In the contractual context, a threat is characterized as an "imminent and serious threat of an act… which it is wrongful to use as a means to obtain the conclusion of the contract."[78] In privacy decision-making, data controllers rely on persuasive – sometimes threatening – language to push data subjects to consent or renounce their privacy. Often, the threat involves being unable to continue using the service in case consent, or additional personal data is not provided. Despite having a softer meaning than the category in the civil law context, pressure to consent or to share more personal data, especially in an environment of extreme asymmetry, directly harms the privacy decision-making process involved.

Second, the idea of "excessive benefit or unfair advantage" was translated as "hindrance."[79] The essential idea is that data controllers are in a position of extreme advantage over data subjects,

---

[76] For further study on the elements and validity of consent, see Nancy Kim, *Relative Consent and Contract Law*, 18 NEV. L.J. 165 (2017).

[77] According to Article 4:108 of the PECL, "A party may avoid a contract when it has been led to conclude it by the other party's imminent and serious threat of an act: (a) which is wrongful in itself, or (b) which it is wrongful to use as a means to obtain the conclusion of the contract, unless in the circumstances the first party had a reasonable alternative."

[78] *Id.*

[79] According to Article 4:109 of the PECL, "(1) A party may avoid a contract if, at the time of the conclusion of the contract: (a) it was dependent on or had a relationship of trust with the other party, was in economic distress or had urgent needs, was improvident, ignorant, inexperienced or lacking in bargaining skill, and (b) the other party knew or

for having knowledge of data practices that are not usually available to data subjects and access to skillful designers that can manipulate the language and interface as wished. Controllers are aware of this imbalance and often use it for their own benefit, in this case, by hindering and making it difficult for data subjects to have access to and express their privacy preferences in a clear and straightforward friendly way. Given data subjects' inexperience and general inability to navigate complex, misleading, and even tricky settings, they are hindered, and their decision-making is negatively impacted.

Third, the idea of "mistake" was translated as "mislead" [80] and covers situations in which the data controller frames the interface, or the information being transmitted to the data subject, in a misleading way to create a wrong understanding of the type of decision-making involved. The data subject will essentially commit a mistake and decide/act in a way that is not the most beneficial for their privacy.

Lastly, the concept of "fraud" was translated as "misrepresent."[81] Here, in the data protection context, the controller benefits from a lack of accountability or stricter regulation to misrepresent facts to the data subject, such as the necessity of certain personal data to perform a task or use the service, the potential experience improvement after the data subject shares more or

---

ought to have known of this and, given the circumstances and purpose of the contract, took advantage of the first party's situation in a way which was grossly unfair or took an excessive benefit."

[80] According to Article 4:103 of the PECL, "(1) A party may avoid a contract for mistake of fact or law existing when the contract was concluded if: (a)(i) the mistake was caused by information given by the other party; or (ii) the other party knew or ought to have known of the mistake and it was contrary to good faith and fair dealing to leave the mistaken party in error; ..., and (b) the other party knew or ought to have known that the mistaken party, had it known the truth, would not have entered the contract or would have done so only on fundamentally different terms."

[81] According to Article 4:107 of the PECL, "(1) A party may avoid a contract when it has been led to conclude it by the other party's fraudulent representation, whether by words or conduct, or fraudulent non-disclosure of any information which in accordance with good faith and fair dealing it should have disclosed."

more in-depth data, or the supposed existence of a legal exception that would authorize a certain privacy practice, when none of these are present.

Below, I present the four categories and their examples. The titles given to each example aim to summarize the characteristics of the respective DPP and facilitate comprehension. The overall goal of the proposed taxonomy is to help us better understand and address the legal challenges behind DPPs, especially how designers negatively affect data subjects' decision-making process. The taxonomy I offer below was cited with acceptance by the European Commission's and the Organization for Economic Cooperation and Development (OECD)'s reports on dark patterns.[82]

A) Pressure

Description: pressuring the data subject to share more personal data (or more in-depth) than intended to continue using a product or service.

Examples:

1. pressure to allow permissions: not allowing the use of a service unless multiple permissions are conceded (*i.e.*, access to the camera, microphone, GPS, contact list and storage in a photo app).

2. *pressure to receive marketing:* requiring the data subject to check the box "receive marketing offers per email" to conclude a purchase or sign up.

---

[82] European Commission, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization,* at 32 (2022): https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418; OECD, *Dark Commercial Patterns*, at 16 (2022), https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en.

3. *pressure to share:* requiring the data subject to reveal personal data to other users in order to use the service (*i.e.* a running app that automatically shares geolocation with other users, not allowing the option to hide it).

4. *pressure to confirm:* using negative persuasive language to make the data subject feel bad about not accepting a certain modality of data collection (*i.e.*, a pop-up window in an e-commerce site that shows two buttons, one saying "yes I want to create a login to gain access to the best offers" and the other saying "no, I do not like offers, I prefer paying a higher price").

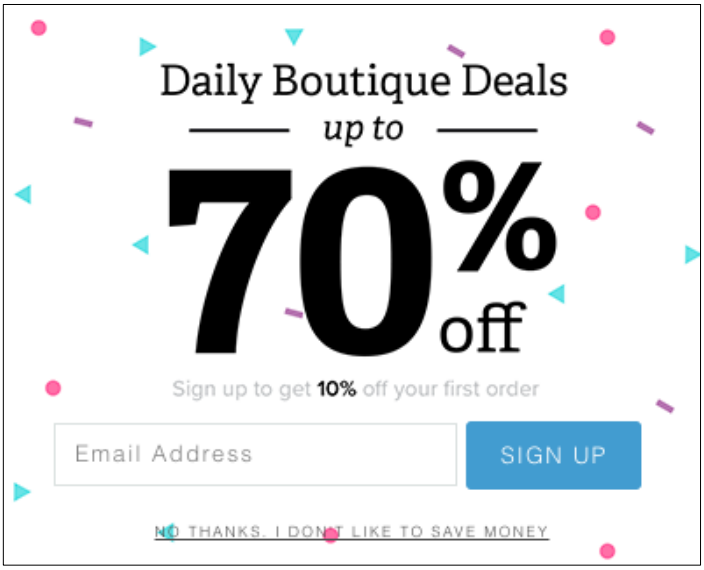

Figure 2.1: an example of *pressure to confirm.* Source: screenshot of the website https://groopdealz.com (browser homepage). After you enter the website, the screen freezes and you see this banner where the sentence at the bottom pressures the user to confirm.

B) Hinder

Description: delaying, hiding, or making it difficult for the data subject to adopt privacy-protective actions.

Examples:

1. *difficult rejection:* consent pop ups that offer the options "accept all" or "more information." If the data subject clicks on the latter, a page with dozens (sometimes hundreds) of green switches appears, containing every entity that currently collects data. Instead of having the option to "reject all," the data subject must go through each switch and turn it off or exit the site.
2. *difficult settings:* privacy settings that are built in a complex and multilayered way, containing various links, explanations, sub-menus, third-party URLs, and other resources to make it difficult (and very unlikely) for the data subject to read and understand.
3. *difficult deletion:* making it difficult (*i.e.*, having to correctly navigate through multiple drop-down choices) or inconvenient (*i.e.*, requiring the data subject to speak with a representative through the phone) to delete the account, occasioning continuous data collection.
4. *privacy-invasive defaults: privacy-invasive defaults (i.e.,* a video social network app that shares videos publicly by default).
5. *hidden settings:* hiding privacy settings in a place that is not intuitive or that the data subject needs to correctly navigate through multiple drop-down choices to arrive.

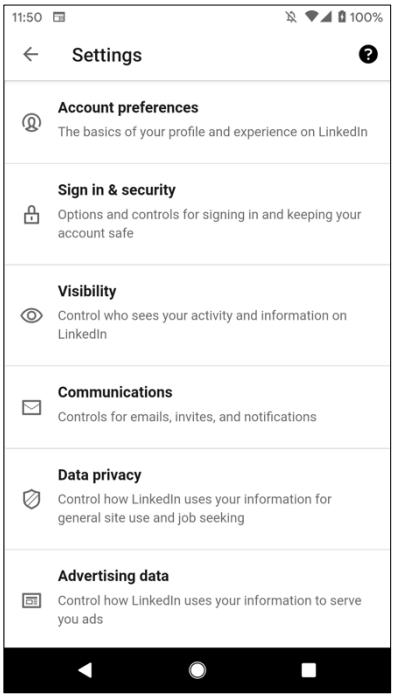

Figure 2.2: an example of *difficult settings*. Source: screenshot of the LinkedIn app, after clicking on the data subject's profile picture and then on "settings." The items "visibility," "communications," "data privacy," and "advertising data" all contain relevant privacy settings. Each of these items contains submenus with additional options and multiple toggles. The data subject would have to review all these dozens of commands to have a comprehensive view of how his personal data is dealt with.

C) Mislead

Description: using language, forms, and interface elements in order to mislead the data subject whilst taking privacy-related actions.

Examples:

1. *ambiguity:* using confusing language such as in a pop-up stating “do not share my data with third parties” with the options “yes” and “no.” It is unclear if ‘yes’ means ‘share’ or ‘do not share.’

2. *double negative:* using double negatives as in “I do not want to deny sharing my data with third parties.” It is difficult for the data subject to understand if he or she should check or uncheck this option in order not to share the data with third parties.

3. *twist:* using colors and symbols in a way that is different than what is customary to misguide the data subject (*i.e.* using green in the “deny” and red in “accept” button or using a the symbol of a padlock beside options that are privacy invasive).

4. *obfuscation:* adding elements to a privacy setting that are not connected to privacy, so that privacy information gets obfuscated.

5. *bad visibility:* using badly contrasted, light colors or small fonts to make privacy-protecting options less visible.

6. framing: describing privacy-invasive features in a positive way to distract the data subject from their downsides.

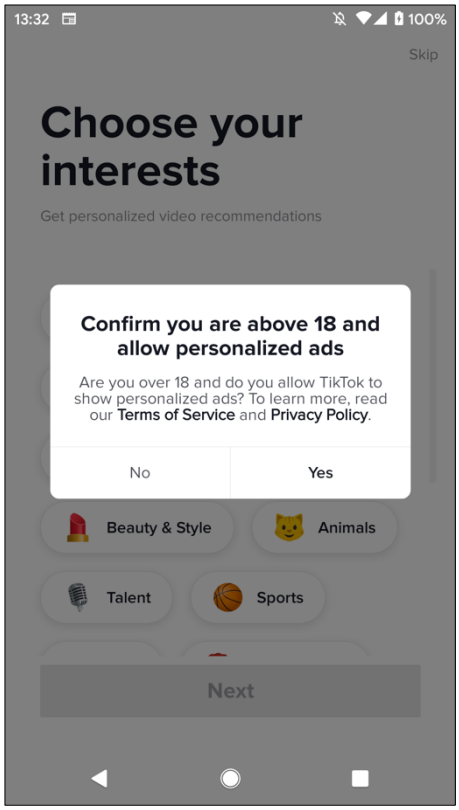

Figure 2.3: an example of *obfuscation*. Source: screenshot of the onboarding experience of a new user on the TikTok app. The question about age is presented together with the question about ad personalization; it is also not clear to which of the questions the buttons “yes” and “no” are referring.

D) Misrepresent

Description: misrepresenting facts to induce data subjects to share more or (more in-depth) personal data than intended.

Examples:

1. False necessity: stating that collecting certain types of data is legally necessary or required for the performance of a task or for system functioning when they are not.

2. False experience improvement: stating that collecting certain types of data is necessary to bring a better experience or a better quality of service when there is no difference to the data subject

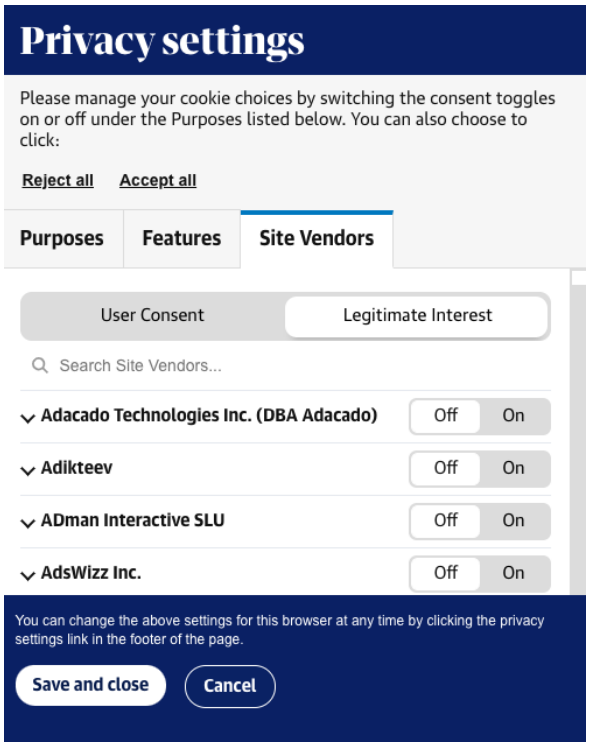

Figure 2.4: an example of *fake necessity*. Source: screenshot from the desktop version of The Guardian newspaper, after clicking on "privacy settings." Targeted advertising by third parties is classified as legitimate interest, which is not true according to the GDPR (it requires consent; only direct marketing can be considered legitimate interest). Additionally, if it was indeed legitimate interest, then consent would not be required (and there are individual consent buttons). The information presented misrepresents the legal requirements.

After discussing cognitive biases and the proposed taxonomy, in the next Section, I turn to data protection law and analyze the current legal status of DPP, especially regarding the GDPR.

VI. DPPs and the GDPR

In this Section, I aim to understand DPPs' legal status in light of the GDPR. More specifically, I inquire (a) whether DPPs fit any of the lawful grounds to collect and process data, and (b) whether there is any rule or principle prohibiting DPP.

The GDPR has various articles dealing with how, why, when, by whom, and for how long personal data may be processed. Moreover, the GDPR's recitals define and explain the principles of data processing, such as transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. They aim to provide guidelines on how personal data should be handled by processors and controllers during the processing phase.

DPPs, however, do not happen in the processing phase. They take place during the collection of personal data on the design interface. The discussion in this Section is, therefore, whether the GDPR has mechanisms to curb manipulative behavior from the controller that happens before data is collected and which leads to it.

Article 6 of the GDPR contains the rules that apply to the collecting phase. Additionally, Article 25 introduces the concept of Data Protection by Design and by Default, which can potentially help set boundaries for design practices. Lastly, the fairness principle, although not defined in the GDPR, is mentioned multiple times, and its philosophical and traditional legal meaning could serve as a key to restraining DPPs. I review each of these options in the following paragraphs.

1. Lawfulness of Data Processing

Article 6 of the GDPR establishes six situations in which data can be lawfully collected and processed. They can be succinctly stated as consent, performance of a contract, legal obligation, vital interest, public interest, or legitimate interest.[83]

Regarding the rules for consent, Article 6(1)(a) establishes that "processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes." To be lawful, consent must be "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[84]

To better understand what these requirements mean, I begin with the condition that consent must be "freely given." According to the GDPR: (a) the data subject should have genuine and free choice,[85] (b) there should not be a clear imbalance between the data subject and the data controller,[86] (c) consent should not be a condition to the performance of a contract,[87] and (d) the data subject should be able to withdraw consent without detriment.[88]

---

[83] GDPR, Article6(1).

[84] GDPR, Article4(11).

[85] Recital 42 of the GDPR states that "(…) consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

[86] Recital 43 of the GDPR puts that "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.(…)"

[87] Article 7(4) of that GDPR states that "when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

[88] Recital 42 of the GDPR states that "(…) consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

The items that are most relevant to the present analysis are (a), (b), and (c) *supra*. As we saw, DPPs rely on cognitive biases to manipulate data subjects to share more or more sensitive personal data. If a DPP negatively interferes with the data subject's decision-making process, consent given under its influence cannot be said to be genuine and represent free choice, such as required by item (a) as the elements that have been manipulated by the controller are not under the awareness of the data subject.

Moreover, there is an important cognitive imbalance between data controllers and data subjects, contrary to what item (b) foresees. Controllers and their designers have the technical ability and the *know-how* to steer the decision-making process of the data subject in a desired direction. On the other hand, data subjects are usually not aware of the topic of cognitive biases and how they can be systemically manipulated by service providers.

Additionally, it is also important to comment that some DPPs infringe item (c), such as "*pressure to receive marketing:* requiring the data subject to check the box 'receive marketing offers per email' to conclude a purchase or sign up," which is the second example I gave in the taxonomy regarding category "Pressure." In these cases, consent would infringe specific GDPR tenets.

A second requirement for consent that is relevant to the present article is to be "informed." According to the GDPR, "for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."[89] DPPs seem not to be affected by this requirement. Controllers usually inform, at some point, data subjects about their identity and the general purposes of the processing for which the personal data is intended and, in another moment, they implement DPPs to collect the desired data.

[89] Recital 42 of the GDPR.

As data subjects tend not to read written declarations, especially long and complex ones, this information will not be properly noticed, and controllers will have a free pass to exploit cognitive biases through the manipulation of interface design.

Given this analysis, DPPs are incompatible with the various consent requirements established by the GDPR. However, more research and public advocacy on the characteristics of dark patterns in privacy and their unlawfulness are needed to pave the way to better enforcement and prevention of DPPs.

This article aims to fill this gap. I propose a taxonomy and a legal definition for dark patterns in privacy and offers a thorough analysis of their characteristics and main manifestations. With increased awareness about practices that should be classified as DPPs - and therefore deemed illegal in case they are deployed to obtain consent or to negatively affect the decision-making process – hopefully, courts, lawmakers, privacy professionals, and the public at large will move towards a more stringent view on the limits of lawful consent.

As of 17 February 2024, the Digital Services Act (DSA) applies in the EU to all platforms within its scope, and it defines and prohibits dark patterns according to the way they define it in Recital 67:

> "Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices 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. Providers of online platforms should therefore be prohibited from deceiving or nudging recipients of the service and from distorting or impairing the autonomy,

> decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof. This should include, but not be limited to, exploitative design choices to direct the recipient to actions that benefit the provider of online platforms, but which may not be in the recipients' interests, presenting choices in a non-neutral manner, such as giving more prominence to certain choices through visual, auditory, or other components, when asking the recipient of the service for a decision."

Despite covering dark patterns in Recital 67, Article 25 of the DSA states:

> "1. Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.
>
> 2. The prohibition in paragraph 1 shall not apply to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679."

Given that paragraph 2 specifically excludes practices covered by the GDPR – such as the DPPs discussed in this article – it seems that the DSA definition and prohibition do not affect the data protection realm.

In the United States, the California Privacy Rights Act (CPRA) which amended the California Consumer Privacy Act (CCPA),[90] added a specific rule that made consent obtained through dark patterns invalid. It established that:

> "(h) 'Consent' means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent."[91] (emphasis added, L.J.)

It is the first time that data protection legislation expressly states that an agreement obtained through dark patterns does not constitute consent. The CCPA represents an important advancement for privacy law, first because the terminology of dark patterns – which stems from interface design – was imported into the privacy realm and helps to better shape and identify design practices that can negatively impact privacy rights. Second, California hosts an important tech hub, and it is

[90] Cal. Civ. Code § 1798.140(h).

[91] *Id.*

where some of the tech giants' headquarters are located. Therefore, legislation affecting them may have a wider national and global effect.

However, it must be noted that, as discussed in this article, DPPs do not only affect consent notices or situations in which the data subject must consent or not. As I have demonstrated, cognitive biases can be exploited in multiple contexts, therefore making data subjects share more or more sensitive data. To cite an example, in the case of extremely complex privacy settings offering dozens or sometimes hundreds of privacy options and granulated choices, there is no consent needed, and the data subject might never discover that those settings exist and never engage with them. Alternatively, the data subject might try to configure each of these settings but give up, given the amount of effort needed. In both cases, the data subject was impacted by a DPP (from the "hinder" category, according to the classification I proposed in this article). However, as there was no consent expected or required, these dark patterns would not be covered by the CCPA.

Mentioning dark patterns in legislation is a first step, as the DSA and the CCPA have done, especially as it helps inform, educate, and generate awareness about the topic. However, both legislations, despite their broad scope and influence, fail to see dark patterns as a broader phenomenon, which involves the exploitation of cognitive biases and structural information and power asymmetries in an interdisciplinary way.

2. Privacy by Design

Another concept that might help to deal with the legality of DPPs is Privacy by Design (PbD),[92] as advanced by Ann Cavoukian. It was absorbed by the GDPR as Data Protection by Design and by Default (DPbDD) and it is expressed in Article 25:

> "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."[93]

Recital 78 of the GDPR specifies what it means with "appropriate technical and organizational measures:"

---

[92] The seven foundational principles of Privacy by Design, as idealized by Ann Cavoukian, the former Information and Privacy Commissioner for Ontario, Canada, are: "1. Proactive not Reactive, Preventative not Remedial; 2. Privacy as the Default Setting; 3. Privacy Embedded into Design; 4. Full Functionality – Positive-Sum, not Zero-Sum; 5. End-to-End Security – Full Lifecycle Protection; 6. Visibility and Transparency – Keep it Open; and 7. Respect for User Privacy – Keep it User-Centric." Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices*, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

[93] GDPR, Article25.

> "(…) such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."

Article 25 and Recital 78, when approaching DPbDD, focus mostly on the processing phase and measures that could be taken to reduce harm in this context, such as data minimization and pseudonymization. As we saw, DPPs happen in the moment of collection of personal data and within the design interface. Without a clearer connection between DPbDD tools and possible measures to be undertaken by controllers to avoid DPPs, it is unlikely that this framework might help curb dark patterns in privacy.

PbD / DPbDD are broad and overarching approaches that can help organizations to design products and services in a more privacy-protective way.[94] However, precisely because they are not

[94] "Privacy by design" consists of a number of principles that can be applied from the onset of systems development to mitigate privacy concerns and achieve data protection compliance. However, these principles remain vague and leave many open questions about their application when engineering systems."- Seda Gürses, Carmela Troncoso, Claudia Diaz, *Engineering Privacy by Design*, PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON COMPUTERS, PRIVACY & DATA PROTECTION, 1 (2011).

technology-specific, for them to be effective in the context of DPPs, further developments need to be made regarding what measures, how, and when should be applied by controllers, as well as the best paths for enforcement and prevention.

3. The Fairness Principle

The GDPR has numerous principles regarding the processing of personal data, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.[95] All these principles are clarified either by the GDPR Articles or by its Recitals, with one glaring exception: the fairness principle.[96]

Fairness is a complex concept. From H. L. A. Hart[97] to John Rawls,[98] different authors have attempted frame and contextualize it. In the legal realm, it has been linked to justice and equality,[99] the absence of discrimination,[100] and reasonableness,[101] and various fields have connected the idea of fairness to specific meanings and standards.[102]

---

[95] GDPR, Article 5(1)(a) et seq.

[96] Fairness is mentioned in Articles 5, 6, 13, 14 and 40 and in Recitals 4, 39, 42, 45, 60, 71 and 129.

[97] H.L.A. Hart, *Are There Any Natural Rights?* 64 PHILO. REV. 175 (1955).

[98] John Rawls, *Justice as Fairness*, 67 PHILO. REV. 164 (1958).

[99] *Id.*

[100] Belinda Smith, *Fair and Equal in the World of Work: Two Significant Federal Developments in Discrimination Law*, 23 AJLL 199 (2010).

[101] Federico Ortino, *From 'Non-Discrimination' to 'Reasonableness': A Paradigm Shift in International Economic Law?*, JEAN MONNET WORKING PAPER N. *01/05* (2005).

[102] Within procedural law, the idea of procedural fairness is central to the validity and quality of the outcome. See Joel Brockner, *Making Sense of Procedural Fairness: How High Procedural Fairness Can Reduce or Heighten the Influence of Outcome Favorability*, 27 ACAD. MANAGE REV. 58 (2002). Within competition law, economic fairness is central to debates in the field, see Alfonso Lamadrid de Pablo, *Competition Law as Fairness*, 8 JECL & PRACT. 147 (2017).

Within EU consumer protection law, for example, the Unfair Commercial Practices Directive (UCPD) has its own definition of unfair commercial practices,[103] as well as a list of commercial practices that are, in all circumstances, considered unfair.[104] The EU Unfair Contract Terms Directive (UCTD) follows the same model.[105]

Within data protection law, there are no consolidated views or rules on what unfair practices are. According to the United Kingdom's (UK) Information Commissioner's Office (ICO):

> "[i]n general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them (…). Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair. In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually."[106]

---

[103] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, Article5.2 (a) & (b).

[104] *Id.* at Annex I.

[105] Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts. It has a definition of what is an unfair term on its Article 3 and a list of terms which are regarded as unfair in its Annex.

[106] Information Commissioner's Office, *Principle (a): Lawfulness, Fairness and Transparency*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/principles/lawfulness-fairness-and-transparency.

This understanding is relevant to the present analysis because it allows us to integrate the idea of interface design manipulation with fairness in data protection. The ICO's definition is based on a philosophical interpretation and does not necessarily have a GDPR legal basis to rely on. For the ICO, the idea of fairness involves handling personal data in a way that: (a) respects the reasonable expectations of data subjects; (b) does not bring adverse effects to data subjects; (c) does not involve deception or misleading the data subject in the moment of collection of personal data; and (d) considers how it affects individual and collective interests of the concerned data subjects.

Based on the preliminary consideration above, DPPs breach the principle of fairness, for cumulatively: (a) not respecting reasonable expectations of data subjects, (b) bringing negative adverse effects to data subjects' decision-making ability, (c) involving manipulation and exploitation of cognitive biases at the time of data collection, and (d) negatively affecting data subjects' privacy.

In this author's view, fairness is a key concept to curb dark patterns in privacy. It allows us to focus on the important elements raised by the ICO, which are the reasonable expectations of data subjects, the practical effects on data subjects, the existence of deception at the moment of collection of personal data, and the individual and collective rights affected by these practices. All these elements are not connected to a specific technology or to a specific rule on how data must be collected. They embrace the idea that it does not matter the shape or form of the technology or practice; the focus should be on the data subject: an individual with expectations, cognitive biases (therefore manipulable), and dignitary rights.

*

In this Section, I inquired whether DPPs could be tackled by (a) the GDPR rules on the lawfulness of data processing, (b) PbD/DPbDD, and (c) the fairness principle. Regarding (a), despite DPP being incompatible with the various consent requirements established by the GDPR, the framework to define, characterize, and repel DPPs still needs to be further developed so that they can be routinely identified and curbed. The DSA and the CCPA might serve as inspirations for practical steps to move forward. Regarding (b), these concepts do not seem to currently fit as mechanisms to stop the spread of DPPs, as more concrete standards and guidelines would need to be put in place – and perhaps this determinacy would go against the nature of PbD and DPbDD themselves. Lastly, regarding (c), there is currently no clarification on what the EU data protection law's approach to the fairness principle is in practice. The GDPR does not define it, and official documents from EU data protection supervisors do not clarify its practical meaning and role within data protection law.

In the next Section, I discuss a necessary change in the decision-making paradigm that supports data protection legislation. When the law starts reflecting a more accurate depiction of the data subject's cognition and behavior, legal principles and rules may be more effective in curbing novel manipulative practices and protecting privacy.

VII. Homo economicus vs Homo manipulable

By applying cognitive psychology to the traditional economic model of rational decision-making, as reflected by the *Homo economicus*,[107] the idea of bounded rationality gained strength.[108] It conveys that cognitive limitations such as biases affect the decision-making process and render the rational-agent model unrealistic.[109]

Bounded rationality is one of the basic assumptions of behavioral economics, which brings the understanding of cognitive psychology to the realm of economics.[110] Gintis proposed that the "*Homo economicus* is replaced by a more accurate model of individual choice and strategic interaction," and Thaler forecasted that Homo economicus would evolve into *Homo sapiens*.[111]

The understanding of cognitive biases, as explained in Section IV *supra*, and the rejection of the *Homo economicus* model are of utmost importance to this article. As we saw, one of the main characteristics of DPPs is the designer's exploitation of cognitive biases: the designer manipulates data subjects through their cognitive biases, against which the data subject has little or no control. The vulnerability of the data subject and their incapacity to calculate, plan and easily

---

[107] The rational-agent model in the traditional economic theory is "personified" as the *Homo economicus* – the economic man. He has determined preferences, is always self-interested, outcome oriented and "has a rate of time preference that allows him to allocate consumption over time in a consistent manner, reflecting his welfare and his concern for the welfare of future generations." - Herbert Gintis, *Beyond Homo economicus: Evidence from Experimental Economics*, 35 ECOL. ECON. 311, 312 (2000).

[108] "Bounded rationality is a concept proposed by Herbert Simon that challenges the notion of human rationality as implied by the concept of *Homo economicus.* Rationality is bounded because there are limits to our thinking capacity, available information, and time (Simon, 1982)", BEHAVIORAL ECONOMICS, https://www.behavioraleconomics.com/mini-encyclopedia-of-be/bounded-rationality.

[109] Daniel Kahneman, *Maps of Bounded Rationality: Psychology for Behavioral Economics*, 93 AM. ECON. REV. 1449, 1449 (2003).

[110] "[b]ehavioral economics seeks to use psychology to inform economics, while maintaining the emphases on mathematical structure and explanation of field data that distinguish economics from other social sciences." Colin Camerer, *Behavioral economics: Reunifying psychology and economics*, 96 PROC. NATL. ACAD. SCI. USA 10575, 10575 (1999).

[111] Richard Thaler, *From Homo Economicus to Homo Sapiens*, 14 J. ECON. PERSPECTIV. 133, 140 (2000).

avoid DPPs make the *Homo economicus* model strongly implausible – and even wrong – within the data protection realm.

However, currently, data protection law – and here I focus on the EU framework – does not expressly reject the *Homo economicus* model. Taking as an example the GDPR, despite its numerous principles and provisions to guarantee data subjects' rights, it allows consent as one of the possibilities for the lawful processing of data, but it does not prevent manipulation and the exploitation of biases through the interface design, where the data subject first interacts with the data controller.

Despite not expressly endorsing the *Homo economicus* model, the GDPR and the EU data protection framework as a whole, do not deny it or present a different approach that clarifies that cognitive biases exist, and humans are vulnerable to manipulation online. There is indeed a protective framework that includes principles,[112] data subjects' rights,[113] the preference for opt-in instead of opt-out[114] and additional rules for consent.[115] However, despite allowing consent – a typical autonomy-supporting mechanism – the GDPR concomitantly does not protect the data subject against possible downsides or traps associated with it, such as the exploitation of cognitive biases through the interface design of websites and apps, therefore allowing DPPs to flourish.

To curb DPPs, many possibilities could be thought of, including ideas involving technology, the market, public awareness, and law. I am specifically concerned with the legal path, given the lack of legal mechanisms to protect data subjects against various forms of exploitation of cognitive biases which will lead to privacy invasive outcomes.

---

[112] GDPR, Arts 5-11.

[113] GDPR, Arts 12-23.

[114] GDPR, Recital 32 and Article4(11).

[115] GDPR, Arts 7 & 8.

My goal is to rethink the legal framework so that controllers, who are the choice architects in the privacy context, are correctly assigned liability and accountability. First, a new paradigm must be established, one that recognizes that data subjects are manipulable and that, absent rules and principles that curb manipulation, data controllers might exploit cognitive biases to obtain outcomes that are favorable for them, but that impact data subjects negatively.[116]

Data subjects are manipulable, and there are data practices happening at the UX level that are not being captured by existing legal frameworks. Rethinking the premises behind the legal framework, including how the legal framework approaches privacy decision-making and potential flaws during the decision-making process, is an essential step to understanding why unfair practices – such as DPP – abound.

The abuse of cognitive biases that takes place online is especially worrisome, as the negative impact on individuals is aggravated by the structure of the web and the technology market. Online, with only one click—one slip of attention—loads of personal data can be transferred to hundreds of data-thirsty third parties. All this happens invisibly to the data subject's eye but under the surveillance of dozens or hundreds of skilled engineers and marketers through their analytics dashboards.

Currently, the GDPR does not expressly acknowledge the existence of cognitive biases or assumptions from cognitive psychology and behavioral economics. It assigns a choice to the data subject and fails to foresee, prevent, and correct all the expected errors in judgment that will be associated with this choice.

---

[116] Data controllers are companies in the pursuit of profit. Exploiting biases help data collection and more data can directly translate into profit through the advertising market. Therefore, absent constraints, data controllers will engage in the exploitation of biases.

It might be said that there are other safeguards to protect privacy and that choice is just part of the data protection framework offered by the GDPR. However, choice opens the door to the data controller, giving it leeway to access personal data. Additional rules modulate how, when, and by whom these data can be used, but the threshold of protection will be definitely lower if the controller can start with a greater amount of data that was potentially extracted from the data subject in a manipulative way.

To curb DPPs and to properly safeguard data subjects, data protection law must embrace the *Homo manipulable,* an individual who is affected by multiple cognitive biases and who is vulnerable to manipulative practices, especially in the online context.

VIII. Conclusion

A DPP is defined in this article as "an interface design choice that manipulates the data subject's decision-making process in a way detrimental to their privacy and beneficial to the service provider."

In this article, I presented the premises, privacy theories, the cognitive biases involved, a proposed taxonomy, the legal status of DPPs within EU data protection law, and the decision-making paradigm that inspires it. My purpose was to understand (a) how DPPs negatively affect the decision-making process of data subjects, and (b) why this is a source of unfairness and should be curbed by the legal framework.

In a nutshell, the GDPR is silent about the exploitation of cognitive biases, manipulative interface designs, and negative interferences in the decision-making process. It also misses the

opportunity to unpack the fairness principle and to present occasions in which unfair practices could spread within the data protection realm, for example, through design.

When building user interfaces, acknowledging cognitive biases and the preventive and corrective measures necessary to mitigate them is indispensable. Human choice will never be perfect; however, in the online environment, any asymmetry is aggravated by the immense processing and analytical powers owned by technology companies. Cognitive biases must be taken for granted, and any choice or interaction framework must overcome them.

As we saw, although the GDPR definition of data processing includes the collection phase,[117] currently, the GDPR ignores important aspects that would ensure broader data subject protection, such as the existence of cognitive biases and the data subjects' vulnerability to manipulation. However, regarding the data collection phase, the one that is affected by the exploitation of cognitive biases, it is almost unregulated, leaving the data subject vulnerable to manipulation.

Interface design practices cannot be ignored. They must embody data protection values and, most importantly, fairness. The interface must reduce, not amplify, the asymmetry between data subjects and controllers.

To curb DPPs, fairness is a central concept, as it reflects the need to balance the asymmetries between controllers and data subjects. The GDPR refers to fairness multiple times, yet it has no definition thereof, either specificity or enforceability for the concept.[118] The way to

---

[117] GDPR, Article4 (2): "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[118] The GDPR refers to fairness or fair processing in five articles (5, 6, 13, 14, 40) and five recitals (38, 42, 45, 60, 71), however, there is no definition or specification of what it means.

advance data protection law is by unpacking the idea of fairness so that it can foster the reduction of asymmetries between controllers and data subjects and support practical ways to implement autonomy and user empowerment.