Do Cognitive Biases and Dark Patterns Affect the Legality of Consent Under the GDPR?

Joanna Taneva
Utrecht University
Amatas
Sofia, Bulgaria
e-mail: joanna.taneva@amatas.com

***Abstract*—Cognitive biases are ever-present in the data subject's decision-making in relation to consent to online tracking. However, the exploitation of cognitive biases via dark patterns can render the obtained consent illegal. This paper aims to combine a variety of legal sources in order to evaluate the legality of consent attained through consent banners. It further provides recommendations on how to resolve this issue in the form of: abolishing the presumption of rationality in data subjects; illustrating the need for more research into the extent to which cognitive biases affect the usability of consent; and normative recommendations for data protection authorities. The results from this study can aid web developers to strive towards designing compliant consent banners.**

Keywords- cognitive bias; consent; consent banners; GDPR; data protection.

I. INTRODUCTION

Currently, most websites collect personal data in order to profit from selling these data to third parties. The ePrivacy Directive (ePD), under Art.5(3), requires the data subject's consent for any storage of tracking technologies on their device [1]. In addition, the General Data Protection Regulation (GDPR) imposes legal requirements for valid consent [2]. Unfortunately, there are no formal requirements as to how consent should be obtained by websites. Recital 17 ePD stipulates that consent can be given by any appropriate method as long as it is "*a freely given, specific and informed indication of the user's wishes".* Consent banners have quickly become the norm where personal data are being processed by websites. They are an inseparable part of the data subject's daily web browsing activities. Research shows it would take the average data subject 244 hours per year to read every privacy policy they encounter on each website they visit [3]. It is argued that data subjects have developed coping mechanisms to deal with the burden of consent banners [4]. Data subjects are prone to deviations from rationality in their decision-making [5, p.1]. This opens the possibility for exploitation of data subjects' decisions via unfair practices such as dark patterns.

The existing literature on cognitive biases and dark patterns shows their potentiality to affect online users' decision-making. However, no assessment of the extent to which exploitation of cognitive biases via dark patterns can affect the legality of consent obtained through consent banners has been made. This paper aims to provide such an assessment.

Section II provides the legal background regarding consent to tracking technologies. Section III provides definitions of cognitive biases and dark patterns. Section IV introduces the immediate gratification bias, maps it to dark patterns and to the GDPR valid consent requirements. Section V follows the same approach in relation to the information overload bias. Section VI provides concluding remarks and recommendations.

II. LEGAL BACKGROUND

Since the right to the protection of personal data is a fundamental right governed by Art. 8 of the European Charter of Fundamental Rights and Art. 8 of the European Convention of Human Rights, any online personal data processing must comply with the existing privacy legislation to safeguard this right [6][7]. Therefore, in the European Union, any use of tracking technologies that process personal data must be compliant with the ePD and the GDPR [8, p.96]. Under Art.5(3) ePD, the use of tracking technologies is only permitted when the user *"has given his or her consent"*. The validity of consent is always assessed under the GDPR according to Art. 2(f) ePD. This is because the GDPR acts as *lex generalis*. It lays down the general rules regarding consent to tracking technologies, while the ePD acts as *lex specialis* – it particularises the general rules of the GDPR in relation to tracking technologies [9, p.13].

Art. 4(11) GDPR defines "consent" as *"any 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"*.

Research by Santos et al. [8] provides a comprehensive analysis of the consent requirements by grouping them into several high- and low-level requirements. The legal consent requirements classification from Santos et al. [8] will be used in this paper because it provides an in-depth analysis which does not merely consult the GDPR legal provisions and EU case law but also secondary sources such as Data Protection Authorities' (DPA) decisions and guidelines. Santos et al. [8] derive an additional "readable and accessible" consent requirement from Art. 7(2) GDPR, which states that consent requests must be *"clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."* Additionally, consent must always be revocable under Art. 7(3) GDPR [8].

 ISBN: 978-1-68558-007-0

III. COGNITIVE BIASES AND DARK PATTERNS

To cope with the vast amount of information presented to them daily, data subjects deploy cognitive heuristics to aid their decision-making [10, para 33]. Cognitive heuristics do not require an assessment of a situation in its full intricacy but rather help the data subject arrive at a quick decision with minimum effort by ignoring part of the information presented [5, p.4][11, p.451]. According to Kahnemann's dual-process theory, the mind has two modes: a fast, heuristics-based system and a slow, rational system. The fast system leads to automatic decisions, such as when asking a person what 2+2 equals, people are likely to give an automatic answer. The slow system requires consideration of many factors. An example is *"checking the validity of a complex, logical argument"*. A key element here is that tasks performed through the slow system need attention and cannot be performed if attention is diverted [12].

Cognitive heuristics are generally beneficial because they save people time and mental capacity [13, p.140]. However, cognitive heuristics sometimes lead to cognitive biases. This is because the appropriate decisions are sometimes incorrectly weighted against the consequences [14, p.2]. Cognitive biases have been defined as a *"systematic (...) deviation from rationality in judgment or decision-making"* [5, p.1]. There are many types of cognitive biases, but this paper merely discusses two cognitive biases – the immediate gratification and information overload bias, which according to previous work affect data subjects' tendency to consent to online personal data processing [15, p.105][16, p.16-19][10, para 34].

Existing literature shows that cognitive biases such as the immediate gratification bias affect data subjects' decision-making by making them underestimate the future consequences of personal data disclosure [17, p.25]. Moreover, research shows that rational privacy decision-making is improbable in an economic sense [17, p.22]. Cognitive biases make rational decision-making more challenging due to design manipulation via dark patterns that often nudge data subjects into taking unintended actions [3, p.105]. Therefore, cognitive biases can be exploited via dark patterns [18]. Previously, legal research has been conducted on the legality of dark patterns in consent banners [19]. However, none of the existing literature examines the legality of the exploitation of cognitive biases through their inevitable interaction with dark patterns.

Recently, the European Data Protection Board (EDPB) issued Guidelines on dark patterns in social media interfaces. Dark patterns are defined there as *"interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions in regards of their personal data"* [20, para 3]. Unfortunately, the EDPB's Guidelines do not apply outside of social media interfaces. The recently adopted Digital Services Act also addresses dark patterns in Art. 23a, however, its application is limited to *"providers of online platforms"* [21]. The Digital Services Act does not provide a classification of the different types of dark patterns. The EDPB Guidelines group the different dark patterns into categories with a definition per each one.

Existing literature shows that dark patterns are not only present in social media but also in manipulative practices regarding consent to online personal data collection [4][19]. Most importantly, the use of dark patterns can lead to the invalidation of consent if any of the valid consent requirements under the GDPR are not met [16, p.15][20].

For the purposes of the ensuing legal analysis, the EDPB Guidelines' classification will be used, as if it applies to all intermediary services, in order to map the cognitive biases to their corresponding dark patterns and to establish whether there are any GDPR valid consent violations.

IV. IMMEDIATE GRATIFICATION BIAS

This section introduces the relationship between the immediate gratification bias and dark patterns in consent banners. It further conducts a brief legal analysis on the legality of the exploitation of immediate gratification.

A. Definition

The immediate gratification bias has been defined as the human propensity to disregard future risks or benefits in favor of immediate gratification. It often comes into play when data subjects browse the web and a consent banner interrupts their browsing activity by asking them to consent to all data processing or tailor their privacy preferences.

Research confirms that cognitive biases, such as the immediate gratification bias, can lead to systematic errors in privacy-related decisions [17, p.24]. As data subjects are prone to underestimating the long-term risks associated with personal data disclosure [10, para 47], they often choose the immediate gratification of accepting all processing purposes as opposed to taking the effort to configure their privacy settings [15, p.105][17, p.25].

B. Mapping to dark patterns

The EDPB's dark pattern named Hindering, with a subcategory called Longer Than Necessary is defined as *"When users try to activate a control related to data protection, the user experience is made in a way that requires more steps from users, than the number of steps necessary for the activation of data invasive options. This is likely to discourage them from activating such control."* [20, p.62].

The exploitation of the *immediate gratification bias* by websites comes into play when only the option to "accept" tracking (or "accept all") exists and no "reject all" option is present in the consent banner interface. Often, data subjects are faced with a consent banner that does not give them the option to reject all trackers but only an option to manually configure their privacy settings on a second or third layer of the banner. An example is Figure 1 below.

The absence of a "reject all" option is a clear example of the interactive superiority of the "accept all" button because data subjects can consent to tracking with one click but can

refuse tracking by having to click at least once more. Additionally, the empirical study by Nouwens et al. found that eliminating the "reject all" button from the initial page of a consent banner increased the likelihood of consent by 22-23% [22, p.8].

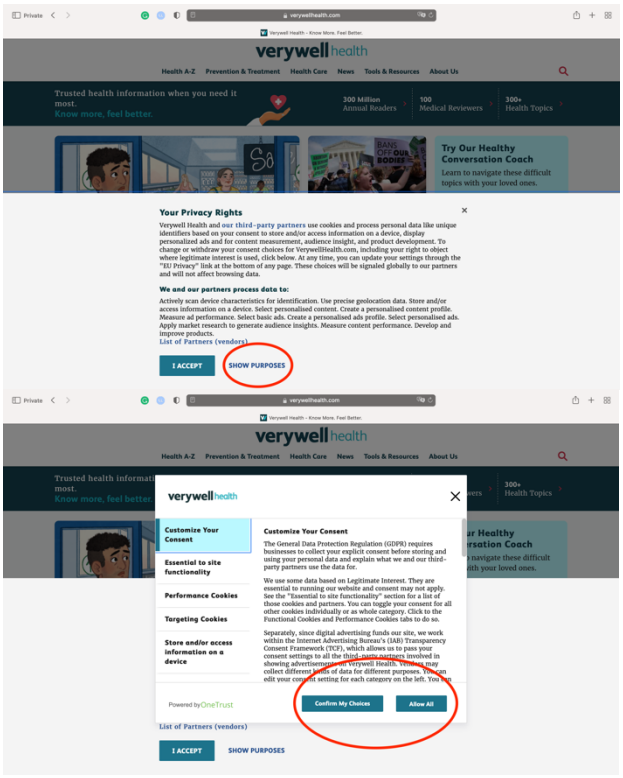

Figure 1. Example of the immediate gratification bias in a consent banner on www.verywellhealth.com accessed on 5 May 2022.

As a result, data subjects prefer to accept privacy-invasive tracking in exchange for immediate access to a webpage [17, p.21].

C. *Mapping to GDPR consent requirements*

According to Art. 4(11) GDPR, as mentioned above, consent must be unambiguous. Santos et al. provide two low-level unambiguous consent requirements called *configurable banner* and *balanced choice* [8]. I argue these low-level requirements are violated when the immediate gratification bias is exploited due to the absence of a "reject all" button.

1) *Configurable banner*

For consent to be unambiguous, there needs to be a clear "yes/no" option according to Article 29 Working Party (A29WP) and several DPAs [8, p.116]. A29WP has phrased this as *"The user should have an opportunity to freely choose between the option to accept some or all cookies or to decline all or some cookies and to retain the possibility to change the cookie settings in the future."* [23, p. 5]. Therefore, this suggests that a requirement for a "reject all" option can be read from Art. 7(3) GDPR, which states that withdrawing consent should be as easy as providing it. Additionally, Recital 66 ePD states that *"The methods of providing information and offering the right to refuse should be as user-friendly as possible."* The EDPB further identifies that when the *Longer Than Necessary* dark pattern is in effect, this leads to a violation of Art. 7(3) GDPR [20, p.62].

Also, if consent can be collected only through one mouse click, data subjects should be able to refuse data processing just as easily [23, p.2]. This view is further shared by the Italian DPA, which states that the mechanism for refusing consent should be *"as user-friendly and accessible as the one in place for giving one's consent."* [24]. Moreover, the French DPA issued a decision against Facebook because it did not provide a "reject all" option. It was ruled that the method for refusing consent must have *"the same degree of simplicity as the method envisaged for accepting"*. Moreover, *"the mere presence of a "Settings" button in addition to the "Accept all" button tends, in practice, to deter refusal and therefore does not allow compliance with the requirements laid down by the GDPR*" [25, paras 90&44].

2) *Balanced choice*

Balanced choice was interpreted from Art. 7(3) GDPR, which states that withdrawing consent must be as easy as giving it [8, p.117]. Therefore, the choice to accept or refuse tracking must be equivalent. In his Opinion on *Planet49*, AG Szpunar suggests (while referring to accepting and refusing cookies) that *"Both actions must, optically in particular, be presented on an equal footing."* [26, para 66]. While this specifically refers to the visual superiority of the "accept all" option over the "reject all" option, it can be argued that it refers to its interactive superiority as well. In other words, the "accept all" and "reject all" options must be interactively equivalent. This view is shared by the Greek DPA, which states that "*The user must be able, with the same number of actions ("click") and from the same level, to either accept the use of trackers (those for which consent is required) or to reject it…"* [27].

Consequently, if no "reject all" button is provided and data subjects must click more than once to reject data processing, this means that manipulation via Hindering: Longer Than Necessary is taking place. This is further evidenced by the fact that user experience research has shown that users spend no more than a minute on websites and that 93.1% of users faced with consent banners stop at the first layer of the interface [28][22, p.8]. Therefore, the absence of a balanced choice violates the requirement for unambiguous consent.

3) *Freely given*

Placing the mechanism to refuse consent at the second layer of a consent interface amounts to a subversion of the data subject's will because it obstructs the exercise of their free will by making the mechanism for accepting consent more user-friendly.

 ISBN: 978-1-68558-007-0

The EDPB specifies that *"free" implies real choice and control for data subjects"* in its discussion of freely given consent [29, para 13]. The French DPA confirms this by stating that *"By applying this requirement of freedom of consent to cookies, it considers that making the optout mechanism more complex than the method allowing them to accept cookies, for example, by relegating to a second window the button allowing them to refuse cookies, amounts in actual fact, in general terms, in the context of browsing on the Internet, to altering users' freedom of choice by encouraging them to favour acceptance of these cookies rather than their refusal."* [25, para 97]. The use of dark patterns strips data subjects of their agency because it interferes with their ability to exercise control of their decisions. This is done in various ways, but it mostly relates to a nudge towards the use of their heuristics-based system via an exploitation of the online choice architecture of consent banners. This includes exploiting both the visual design and the language used in consent banners. Accordingly, this exploitation clashes with the notion of freely given consent [30, p.10]. The EDPB refers to the Norwegian Consumer Council and it states that *"Dark patterns aim to influence users' behaviours and can hinder their ability "to effectively protect their personal data and make conscious choices", for example by making them unable "to give an informed and freely given consent"* [20, p.7].

V. INFORMATION OVERLOAD BIAS

This section introduces the relationship between the information overload bias and dark patterns in consent banners. It further conducts a brief legal analysis on the legality of the exploitation of information overload.

A. Definition

When humans are faced with substantial amounts of information that they must read to reach a certain decision, information overload may occur. This means they are more likely to dismiss the presented information entirely as opposed to filtering out the important parts [16, p.16]. The information overload bias comes into play when a data subject is flooded with information regarding the processing of their personal data in a consent banner, which renders selecting the privacy-friendly settings even more difficult [10, para 34]. Literature shows that consent is highly dependent on the "cognitive load" imposed on data subjects, and if they are overburdened with information, it increases the likelihood of them giving consent to personal data processing [10, para 34].

B. Mapping to dark patterns

The use of the information overload bias by websites in consent banners can be correlated with the dark pattern the EDPB has classified as Overloading. The relevant subcategory of this dark pattern is called Too many options and is defined as *"Providing users with (too) many options to choose from. The amount of choices leaves users unable to make any choice or make them overlook some settings, especially if information is not available. It can lead them to finally give up or miss the settings of their data protection preferences or rights."* [20, pp.60-61].

An example of the information overload bias in practice is shown in Figure 2 below. In the example we can see 8 adjustable toggles to enable data collection. When the question mark button is clicked a brief explanation for each purpose is displayed. The consent banner, when visited through the website, contains more than 20 adjustable toggles. As previously mentioned, data subjects do not spend more than a minute on a webpage [28]. It is apparent how presenting the data subject with this many options leads to information overload.

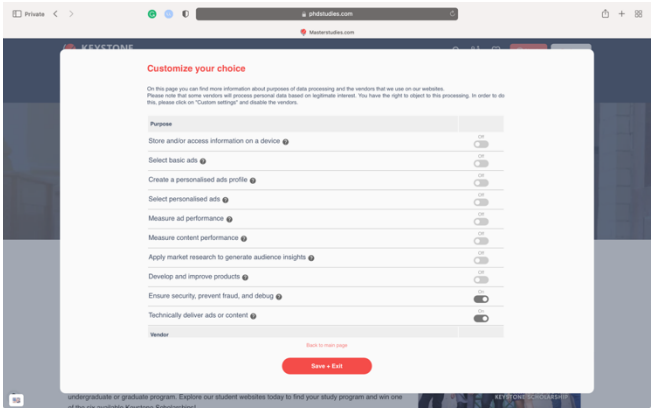

Figure 2. Example of the information overload bias in a consent banner from www.phdstudies.com accessed on 5 May 2022.

C. Mapping to GDPR consent requirements

1) Informed

AG Szpunar ruled informed consent implies that the data subject understands the consequences of the processing [31, para 47]. The CJEU further ruled in *Planet49* that the information provided must be *"clearly comprehensible and sufficiently detailed so as to enable the user to comprehend the functioning of the cookies employed"* [32, para 74].

If data subjects cannot make an informed decision, as previously evidenced by behavioral research findings, due to being overloaded with information [33, p.76], and due to their inability to read all the processing information available in consent banners and privacy policies [34, p.68][15, p.104][33, p.75], then consent cannot possibly be informed under Art. 4(11) GDPR. This leads to the invalidity of consent as a legal basis and to unlawful data processing.

Data subjects must understand what will happen to their data and what the outcome of using their data will be. For example, data subjects need to understand that consenting to targeting cookies may lead to them being exposed to personalized advertisements. The Belgian DPA has ruled that when the user had to follow the policies of 449 vendors, providing informed consent was *"illusory and impracticable"* [35, p.7].

Overloading data subjects with information nudges them into using their fast, heuristics-based system. The large amount of time they would have to spend informing themselves about the different processing purposes and their consequences imposes a high transaction cost. Data controllers provide data subjects with information regarding personal data processing, and the time data subjects spend reading this information is considered the transaction cost. High transaction costs obstruct data subjects from making a rational decision, which is why they are likely to disregard informing themselves about the data processing and are more likely to click consent [36, p. 31].

2) Readable and accessible

Pursuant to Recital 32 GDPR, a consent request must be *"clear, concise and not unnecessarily disruptive to the use of the service for which it is provided"*.

"Clear and concise"

Art. 13 GDPR imposes informational requirements on data controllers when personal data are being collected from data subjects. Art. 12 GDPR imposes requirements on the modalities through which that information is provided to data subjects. Art. 12(1) GDPR provides *"The controller shall take appropriate measures to provide any information referred to in Articles 13 [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form…"*. In a discussion of Art. 12(1) GDPR and its requirement for *"concise"* information, A29WP has recommended that *"data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue."* [37, para 8]. Information fatigue is also known as information overload. It was first presented by the sociologist Georg Simmel, who introduced the theory that the overload of sensations in the urban setting made people indifferent and prevented them from logical reactions [38]. Presenting data subjects with too much information is a violation of the requirement for *"concise"* consent requests because it leads to information fatigue. As previously discussed, data subjects do not spend more than a minute on a webpage [28]. This makes it even more apparent how information fatigue is very likely to occur because of the amount of time an average person spends on a webpage and the amount of information they have to process in that minute.

VI. Conclusion and Future Work

The current data protection legal framework needs to be amended and supported with best practices to sufficiently protect data subjects against the exploitation of their vulnerabilities. While it gives data subjects control over their personal data (i.e., the right to decide whether to consent to tracking), it does not protect them against exploitation of the mechanisms used to obtain consent [18, p.48]. Therefore, the following recommendations are provided so that the validity of consent can be improved.

The presumption of rationality in data subjects is wrong. The GDPR imposes on data subjects a presumption of rationality [39]. However, rational decisions are practically impossible given the cognitive load imposed on the data subject. In fact, research has proven that rational privacy decision-making is improbable [17, p.22]. Therefore, the assumption of rationality should be abolished and more emphasis should be placed on cognitive biases and their exploitation via dark patterns in consent banners. Future work from behavioral psychology and behavioral economics research could conduct real-world surveys to examine to what extent cognitive biases affect data subjects' decision-making in relation to accepting tracking via consent banners.

The exploitation of cognitive biases via dark patterns negatively affects the usability of consent. The illegality of the obtained consent leads to an inefficient data protection legal system. A way efficiency could be improved is through increasing the usability of consent banners. There is a need for a contextual interpretation of manipulation via dark patterns that takes into account the human propensity to exhibit cognitive biases. Arguably, this can be achieved through a contextual approach to usability, which considers user needs and limitations, i.e., cognitive biases. More research is needed on the extent to which cognitive biases affect the usability of consent banners. Moreover, research is needed on whether the development of usability tools and usability evaluation methods can improve the usability of consent banners. Future research could also examine whether cognitive biases affect other matters not related to data protection and online consent, such as, for example, users' ability to apply cybersecurity practices, tools and policies.

It is recommended that DPAs issue guidelines on cognitive biases and dark patterns in consent banners, as well as guidance for data controllers on how to achieve valid consent without exploitation. A classification of dark patterns and cognitive biases related to consent will contribute to companies' abilities to recognize and avoid them. Additionally, DPAs could create a set of design principles applicable to consent banners that could standardize their design in order to minimize the possibilities for exploitation of cognitive biases. Furthermore, a way in which it can be ensured that consent banners are not exploiting cognitive biases is conducting usability assessments. Usability assessments can provide scientifically supported evaluations of the extent to which consent banners are compliant with the GDPR consent requirements [40, p.4]. Usability assessments can also aid with the identification of usability problems in the consent banner interface which will further prompt web developers to strive toward GDPR-compliant consent banner design and prevent the exploitation of cognitive biases.

Acknowledgment

The author would like to thank dr. Cristiana Teixeira Santos, Assistant Professor in data protection and privacy law at Utrecht University for her continued support during and after completion of the author's studies. The author would

also like to thank her mother, Antonia Prodanova, for her unconditional love and support.

REFERENCES

[1] Directive 2009/136/EC of the European Parliament and of the Council (of 25 November 2009) amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[2] Regulation (EU) 2016/679 Of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation") OJ 2 119/1.

[3] A. E. Waldman, "Cognitive biases, dark patterns, and the 'privacy paradox,'" Current Opinion in Psychology, vol. 31, pp. 105–109, 2020.

[4] H. Habib, M. Li, E. Young, and L. Cranor, "'Okay, whatever': An Evaluation of Cookie Consent Interfaces," presented at the CHI Conference on Human Factors in Computing Systems, pp. 1-27, 2022.

[5] F. Blanco, Cognitive Bias. Encyclopedia of Animal Cognition and Behaviour. 2017.

[6] European Parliament., & Office for Official Publications of the European Communities, Charter of fundamental rights of the European Union. 2000.

[7] Council of Europe, The European Convention on Human Rights. 1952.

[8] C. Santos, N. Biielova, and C. Matte, "Are cookie banners indeed compliant with the law?," Technology and Regulation, pp. 91–135, 2020.

[9] European Data Protection Board, "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.," 2019.

[10] Y. Hermstrüwer, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data," JIPITEC, pp. 9–26, 2017.

[11] G. Gigerenzer and W. Gaissmaier, "Heuristic Decision Making," Annual Review of Psychology, vol. 62, no. 1, pp. 451–482, 2011.

[12] D. Kahneman, Thinking Fast and Slow, 1st ed. Farrar, Straus and Giroux, 2013.

[13] J. van der Lee et al., "Ethical design: persuasion, not deception.," Journal of Digital & Social Media Marketing, vol. 9, no. 2, pp. 135–148, 2021.

[14] J. E. Korteling, A.-M. Brouwer, and A. Toet, "A Neural Network Framework for Cognitive Bias," Front. Psychol., vol. 9, Art. 1561, pp.1-12, Sep. 2018, doi: 10.3389/fpsyg.2018.01561.

[15] F. Z. Borgesius, "Informed Consent: We Can Do Better to Defend Privacy," IEEE Secur. Priv., vol. 13, no. 2, pp. 103–107, Mar. 2015, doi: 10.1109/MSP.2015.34.

[16] CNIL, "IP Report: Shaping Choices in the Digital World, From dark patterns to data protection: the influence of UX/UI design on user empowerment (No. 6)," Commission Nationale de l'Informatique et des Libertés, 2019.

[17] A. Acquisti, "Privacy In Electronic Commerce And The Economics Of Immediate Gratification", EC'04: Proceedings of the 5th ACM conference on Electronic commerce, pp. 21–29, 2004.

[18] L. Jarovsky, "Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness," SSRN Electron. J., pp.1-50, 2022, doi: 10.2139/ssrn.4048582.

[19] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective," in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama Japan, May 2021, pp. 1–18. doi: 10.1145/3411764.3445779.

[20] European Data Protection Board, "Guidelines 03/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them," 2022.

[21] European Parliament, Position of the European Parliament adopted at first reading on 5 July 2022 with a view to the adoption of Regulation (EU) 2022/… of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. European Parliament. 2022.

[22] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence," in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu HI USA, Apr. 2020, pp. 1–13. doi: 10.1145/3313831.3376321.

[23] Article 29 Data Protection Working Party, "Working Document 02/2013 providing guidance on obtaining consent for cookies," 2013.

[24] Italian DPA, "Guidelines on the use of cookies and other tracking tools – 10 June 2021", Official Journal of the Italian Republic No 163 of 9 July 2021, Garante per la protezione dei dati personali, "Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 [9677876]," 2021. Accessed: Sep. 28, 2022. [Online]. Available: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876#english

[25] CNIL, Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED. 2021.

[26] Opinion of Advocate General Szpunar in Case C 673/17 Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

[27] Greek Data Protection Authority, "Guidelines on Cookies and Trackers," 2020. Accessed: Sep. 28, 2022. [Online]. Available: https://iapp.org/news/a/greek-dpa-issues-guidelines-on-cookies-and-trackers/#:~:text=In%20February%202020%2C%20the%20Hellenic,EU%20General%20Data%20Protection%20Regulation

[28] J. Nielsen and D. Norman, "The Definition of User Experience (UX)." https://www.nngroup.com/articles/definition-user-experience/ (accessed Aug. 26, 2022).

[29] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679," 2020.

[30] Norwegian Consumer Council, "Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy," 2018. Accessed: Sep. 28, 2022. [Online]. Available: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

[31] Opinion of Advocate General Szpunar in Case C 61/19 Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

 ISBN: 978-1-68558-007-0

[32] Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH. 2019.
[33] S. Monteleone, "Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation," Syracuse Journal of International Law and Commerce, vol. 43, no. 1, pp. 69–120, 2015.
[34] S. Y. Soh, "Privacy Nudges:," Eur. Data Prot. Law Rev., vol. 5, no. 1, pp. 65–74, 2019, doi: 10.21552/edpl/2019/1/10.
[35] Belgian DPA v Roularta Media Group Decision 85/2022. 2022. Accessed: Sep. 28, 2022. [Online]. Available: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-85-2022.pdf
[36] F. J. Zuiderveen Borgesius, "Consent to Behavioural Targeting in European Law - What are the Policy Implications of Insights from Behavioural Economics?," SSRN Electron. J., pp. 1-58, 2013, doi: 10.2139/ssrn.2300969.
[37] Article 29 Data Protection Working Party, "Guidelines on transparency under Regulation 2016/679 Rev. 01," 2018.
[38] G. Simmel, "The Metropolis and Mental Life," in The Sociology of Georg Simmel, New York: The Free Press, pp. 409–424, 1950.
[39] A. E. Waldman, "Committee On The Internal Market And Consumer Protection," presented at the Public hearing: Dark patterns and how such practices harm consumers and the Digital Single Market. Accessed: Sep. 28, 2022. [Online]. Available: https://multimedia.europarl.europa.eu/en/webstreaming/committee-on-internal-market-and-consumer-protection_20220316-0945-COMMITTEE-IMCO
[40] T. Jakobi, M. von Grafenstein, P. Smieskol, and G. Stevens, "A Taxonomy of user-perceived privacy risks to foster accountability of data-based services," J. Responsible Technol., vol. 10, p. 100029, Jul. 2022, doi: 10.1016/j.jrt.2022.100029.

 ISBN: 978-1-68558-007-0