Maastricht University
Faculteit der Rechtsgeleerdheid

Maastricht Centre
for European Law

Dark Patterns and Privacy Rights in the Digital Age: Evaluating the GDPR and DSA's Regulatory Responses to Deceptive Designs

Estelle Herbiet

MCEL Master's Thesis Series
No 2025/04

The MCEL Master's Thesis Series seeks to give excellent students the opportunity to publish their final Master's theses and to make their work accessible to a wide audience.

Those wishing to submit papers for consideration are invited to consult our website and to send their work to mcel@maastrichtuniversity.nl.

Published in Maastricht, May 2025

Faculty of Law
Maastricht University
Postbox 616
6200 MD
Maastricht
The Netherlands

This paper is to be cited as MCEL Master's Thesis Series 2025/04

Abstract

This thesis explores the regulation of dark patterns within the European Union legal framework, focusing on the interplay between the General Data Protection Regulation and the Digital Services Act. It examines the challenges and limitations of these regulations in addressing deceptive design practices that manipulate user choices. While the DSA marks a significant step by explicitly prohibiting dark patterns, its effectiveness is constrained by its partial overlap with the GDPR and its reliance on future guidelines. The GDPR, though robust in data protection, does not explicitly cover dark patterns, sometimes creating gaps in protection. The thesis argues for a more unified and targeted regulatory approach to effectively tackle dark patterns and safeguard digital users' privacy.

Acknowledgements

I would like to express my deepest gratitude to the individuals without whom drafting my thesis and completing this advanced master's degree would not have been possible. First, I extend my sincere gratitude to my supervisor, Professor Herke Kranenberg. His invaluable guidance and thoughtful feedback challenged me to write what has become my favourite paper to date, on a topic I feel deeply passionate about.

This journey would not have been possible without my partner, Frederik, whose support since my very first day of law school has carried me through every academic milestone. I am incredibly grateful to have him in my life.

I also wish to thank my close friends: Margarida and Lucy, for the countless hours spent discussing and proofreading this thesis with me; and Maximilian and Julia, for the daily catch-ups, the laughter, and the hourly calls during "exam crisis periods" throughout this LL.M., which brought great comfort and inspiration.

I am deeply indebted to my managers, Mr Lakboune and Mr Daman, for enabling me to pursue this degree alongside my professional responsibilities at the European Parliament and the European Central Bank. Their flexibility and support were instrumental in the successful completion of this degree.

Special thanks also go to my *marraine*, Christine, and my mother, Sylvie. Their unwavering encouragement, thoughtful check-ins, and love were a constant source of strength throughout the thesis journey.

Finally, I am sincerely grateful to all staff members at the European Centre for Privacy and Cybersecurity and Maastricht University. I especially thank Megan Lana, my first lecturer, whose encouragement during my early doubts about law school made all the difference. I am also thankful to Karolina Podstawa, who first introduced me to the world of privacy and data protection. Her teaching sparked a lasting passion in me that has shaped both my academic and professional paths ever since.

As the French saying goes, *On n'est riche que de ses amis* - the only true wealth in life lies in the friends and family we have. I feel incredibly fortunate to have been supported by such generous and inspiring people throughout this journey.

Table of Abbreviations

CJEU	Court of Justice of the European Union, also 'the Court'
DSC	Digital Services Coordinator
DMA	Digital Markets Act
DPA	Data Protection Authority
DPC	(Irish) Data Protection Commission
DPD	Data Protection Directive
DPbD	Data Protection by Design
DPbDf	Data Protection by Default
DSA	Digital Services Act, also 'the Act'
DSC	Digital Services Coordinator
EBDS	European Board for Digital Services
EC	European Commission, also 'the Commission'
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation, also 'the Regulation'
MS	Member State
UCPD	Unfair Commercial Practices Directive
UI	User Interface
UX	User Experience
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine

Table of Contents

1. Introduction

In the digital age, user interface design has become a powerful tool for influencing online behaviour. Dark patterns – deceptive designs that manipulate users into making unintended decisions regarding their personal data – have emerged as a significant concern in the realm of data protection. These manipulative practices are alarmingly prevalent, with nearly 97% of the most popular websites and apps used by European Union (EU) consumers deploying at least one dark pattern.[1] As awareness of dark patterns' detrimental effects grows, regulatory frameworks continue to evolve, aiming to curb these practices and protect consumers.[2] The widespread use of deceptive designs poses a threat to individuals' privacy and data protection rights, undermining the transparency and user autonomy principles that form the cornerstone of modern data protection regulations.

User interface (UI) and user experience (UX), favouring personalised and seamless interactions, often promote behaviours conflicting with data protection. In many data-driven business models, interfaces are designed to maximise data collection, often at the expense of user privacy, which has prompted a shift in the focus from academic discourse to active enforcement by regulatory bodies. In the EU, efforts to combat these manipulative practices are primarily governed by two regulations: the General Data Protection Regulation (GDPR)[3] and the Digital Services Act (DSA).[4] Additionally, the European Data

[1] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) <https://data.europa.eu/doi/10.2838/859030> accessed 30 August 2024, 45 and 120.

[2] This thesis will interchangeably use the terms 'consumers', 'users', 'individuals', and 'data subjects'.

[3] 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) [2016] OJ L119/1.

[4] 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) [2022] OJ L277/1.

Protection Board (EDPB) issued guidelines[5] which clarify how the GDPR applies to dark patterns.

This thesis examines the effectiveness of the GDPR and DSA in regulating dark patterns from a data protection perspective. The central question it aims to answer is whether, and how effectively, dark patterns are regulated under these frameworks. The research will employ a doctrinal analysis of the relevant EU legal frameworks, supported by a review of academic literature and industry guidelines. While the scope of the analysis will focus on the GDPR and DSA, the thesis will briefly contextualise related laws, such as the Unfair Commercial Practices Directive (UCPD).[6] Ultimately, this thesis aims to contribute to systematising and clarifying the current legislation, using legal reasoning to suggest improvements to both the law and industry practices.

The thesis begins by defining dark patterns, their taxonomy, and their impact on data protection. The second chapter examines the GDPR's provisions relevant to regulating dark patterns, including pertinent Court of Justice of the European Union (CJEU) cases. The third chapter introduces the DSA as a recent regulatory development in the EU, outlining its key provisions for regulating dark patterns. Finally, the fourth chapter assesses the effectiveness and limitations of both the DSA and GDPR in addressing dark patterns, exploring their interplay, the legal terms they introduce, and their mechanisms for enforcement and harmonisation. Based on this analysis, the thesis offers recommendations to enhance the data protection framework concerning dark patterns in the EU.

[5] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them' (Version 2.0, February 2023), hereinafter referred to as "European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns'".

[6] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L149/22.

2. Dark Patterns

2.1 Background and Definition

Prior to widespread digitalisation, manipulation and deception techniques were predominantly employed in brick-and-mortar marketing.[7] A contemporary example of physical manipulation and deception techniques being used in physical locations is the 'forced path' layout used in some stores.[8] This design compels customers to walk through a winding corridor from entrance to exit, with no shortcuts available. The path strategically positions retail displays in customers' direct line of sight, ensuring they see the entirety of the store before they can exit.[9] Despite such techniques being known to coerce and manipulate customers, some businesses continue to utilise them as they have shown to boost revenue.[10]

As digitalisation transforms sales and advertising, organisations increasingly utilise deceptive techniques known as dark patterns on their online platforms.[11] The extensive range of design options and enhanced understanding of behavioural insights enable companies to exploit consumer biases more effectively than in face-to-face transactions. As online interactions allow businesses to gather user behaviour data and optimise their practices to influence consumers, the reach and impact of dark patterns online surpass similar offline practices in both scale and cost-effectiveness, facilitating the implementation of manipulative experiences.[12] UI design plays a crucial role in shaping individuals' interactions with technology. Ideally, interfaces should assist users in achieving their intended goals. The design process involves physical, perceptual, and conceptual interactions, with visual elements like

[7] That is, marketing for a business with a physical location.

[8] Examples of such stores are famous Scandinavian brands such as IKEA, Normal, and Søstrene Grene.

[9] Harry Brignull, 'Part One: Diving into the World of Deception', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[10] Aislelabs, 'Customer Paths and Retail Store Layout — Part 3 (*Aislelabs*, 2018) <www.aislelabs.com/blog/customer-paths-and-retail-store-layout-part-3> accessed 30 August 2024.

[11] Tim Kollmer and Andreas Eckhardt, 'Dark Patterns: Conceptualization and Future Research Directions' (2023) 65 Business & Information Systems Engineering 201 <https://doi.org/10.1007/s12599-022-00783-7> accessed 30 August 2024.

[12] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) <https://doi.org/10.1787/44f5e846-en> 12.

layout, colour, font size, and buttons, along with images and text, significantly influencing user behaviour and choices. While achieving a completely neutral design may be impossible, and effects are not always intentional, it is common for companies to deliberately design interfaces that nudge users toward specific, predictable decisions.[13]

The term 'dark patterns' was first coined by Brignull nearly fifteen years ago, who defined it 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".[14] Initially, the term served as a catch-all to describe how UI designs could negatively influence users and their decision-making, as reflected in Brignull's taxonomy. Brignull's original definition and taxonomy, while groundbreaking, have been expanded upon by subsequent research to reflect other types of dark patterns as well as their harmfulness.[15] In 2019, Mathur and others conducted an extensive study analysing 53,000 product pages from 11,000 shopping websites. This research uncovered nearly 2,000 instances of dark patterns.[16] Their research led to a more comprehensive taxonomy and a refined definition of dark patterns as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make".[17]

The above are only two examples of many dark pattern definitions. As is often the case with legal concepts, there is no widely accepted definition of dark patterns, which is also partly owed to the variety of practices referred to as

---

[13] Agnieszka Kitkowska, 'The Hows and Whys of Dark Patterns: Categorizations and Privacy' in Nina Gerber, Alina Stöver and Karola Marky (eds), *Human Factors in Privacy Research* (Springer, Cham 2023) <https://doi.org/10.1007/978-3-031-28643-8_9> accessed 30 August 2024, 174.

[14] Harry Brignull and others, 'Dark Patterns: Deception vs. Honesty in UI Design' (*A List Apart*, 1 November 2011) <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/> accessed 30 August 2024.

[15] Johana Gunawan and others., 'Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions' [2022] CSLAW '22: Proceedings of the 2022 Symposium on Computer Science and Law 181 <https://pure.uvt.nl/ws/portalfiles/portal/65614055/gunawan_santos_kamara_2022_cslaw.pdf> accessed 30 August 2024.

[16] Arunesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3 Proceedings of the ACM on Human-Computer Interaction 1 < https://arxiv.org/pdf/1907.07032.pdf > accessed 30 August 2024.

[17] ibid, 2.

such, and different views on whether certain practices should be considered as dark patterns.[18] Over time, the term has evolved into an umbrella concept encompassing numerous online practices, often referred to as 'deceptive design', 'deceptive pattern', 'deceptive or manipulative patterns', or similar terms. Despite the varying terminology, these practices share a common goal: to steer, deceive, coerce, or manipulate users into making decisions that may not align with their best interests, including those related to their personal data.[19] For the purpose of this thesis, the extensive definition introduced by the EDPB Guidelines on deceptive design patterns[20] will be adopted. According to the EDPB, dark patterns are

> *interfaces and user journeys implemented on platforms that aim to influence users into making unintended, respectively unwilling, and/or potentially harmful decisions, often toward an option that is against the users' best interests and in favour of the platforms' interest, with regard to the processing of their personal data. Deceptive design patterns aim to influence users' behaviours, generally relying on cognitive biases, and can hinder their ability to effectively protect their personal data and make conscious choices, for example by making them unable to give informed and freely given consent. This can be exploited in several aspects of the design, such as interfaces' colour choices and placement of the content*.[21]

This definition encompasses the key elements of dark patterns, highlighting their manipulative nature, the exploitation of cognitive biases, and the specific concern for data protection. By adopting this definition, the thesis aligns with current regulatory perspectives on deceptive design practices in digital interfaces.

Deceptive designs, as indicated by the definitions provided, exploit users' cognitive biases and, possibly subliminally, influence their behaviour. These dark patterns often leverage what is dubbed as 'System 1' thinking, which involves instinctive, automatic decision-making with little cognitive effort, as opposed to the deliberate, conscious, and laborious decision-making

[18] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 8.

[19] ibid, 9.

[20] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns'.

[21] ibid, 9.

represented by 'System 2' thinking.[22] The *intentionality* behind dark patterns is a complex issue. Whilst often deliberately designed, they can also arise unintentionally due to poor design choices, lack of UX awareness, or oversight in the design process.[23] It is crucial to note that not all manipulative designs are dark patterns: designs that nudge users toward protecting their privacy, even if the outcomes may be contrary to their initial preferences, are not dark patterns as they serve a beneficial purpose.[24] Manipulation alone, without malicious intent, does not necessarily constitute a dark pattern. In some cases, businesses aiming to improve growth and performance metrics may inadvertently adopt exploitative practices as a by-product of a larger goal, thereby not recognising their negative impact.[25] However, any design leaving users worse off, intentional or not, should be considered malicious.[26] The prevalence of overtly manipulative dark patterns often suggests intentionality, frequently stemming from exploitative business strategies viewing users as resources rather than partners.[27] This mindset often extends to approaching laws as systems to be exploited for profit, suggesting that deceptive patterns could be a rational response to under-regulated and under-enforced marketplaces.[28]

---

[22] Daniel Kahneman, *Thinking, Fast and Slow* (Farra, Straus and Giroux 2021).

See also OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 9.

[23] For example, a feature might be developed with the aim of enhancing user experience, but if it inadvertently restricts users' control over their personal data or obscures important information, it can function as a dark pattern, even without malicious intent. Business pressure or conflicting priorities can also lead to the unintentional implementation of designs that prioritise data collection or user engagement over transparency and user control.

[24] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN <http://dx.doi.org/10.2139/ssrn.4048582> accessed 30 August 2024, 6.

[25] Harry Brignull, 'Part 5: Stamping out deceptive patterns, Chapter 26: The crucial role of regulation', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[26] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 7.

[27] Harry Brignull, 'Part 2: Exploitative strategies', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[28] Harry Brignull, 'Part 5: Stamping out deceptive patterns, Chapter 26: The crucial role of regulation', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

Dark patterns manifest in diverse forms and designs, influenced by content and interface elements. Content-based patterns focus on wording, context, and information presented, while interface-based patterns involve the display of content and user navigation.[29] These manipulative designs can appear across various digital platforms, including websites, apps, cookie notices, search engines, and online games. They may be encountered at any stage of user interaction, from entry requests to user settings and exit processes.[30] Research has shown that combining multiple dark patterns can increase their cumulative effectiveness, as their interplay can more significantly influence user decision-making compared to individual patterns.[31] Ultimately, these designs coerce individuals into sharing personal information for collection, storage, and processing, often against their original intentions and interests.[32] The following section will explore the different types of dark patterns in more detail.

2.2 Taxonomies and Types of Dark Patterns

2.2.1 Dark Pattern Taxonomies

As the range of practices identified as dark patterns continues to expand, academic research has thus far concentrated on gathering examples and categorising them. However, much like the challenge of establishing a universally accepted definition, it is improbable that a comprehensive and final taxonomy of dark patterns will ever be developed. Indeed, the continuous evolution of new patterns, technologies, and interfaces renders any taxonomy inherently limited and unlikely to be future-proof. Moreover, taxonomies often reflect their authors' objectives, particularly regarding the criteria for including

[29] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 10.

[30] Johana Gunawan and others, 'Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions' [2022] CSLAW '22: Proceedings of the 2022 Symposium on Computer Science and Law 181, 186.

[31] This may result from interactions between the patterns or the increased likelihood that at least one will be effective.

OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 22.

[32] Christoph Bosch, 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' (2016) 4 Proceedings on Privacy Enhancing Technologies 237 <https://doi.org/10.1515/popets-2016-0038> accessed 30 August 2024, 252.

or excluding specific practices.[33] While some taxonomies strive for broad comprehensiveness,[34] others focus on patterns identifiable through web crawling techniques or are tailored to specific policy areas or behaviours, such as online gaming, consumer protection, or privacy.[35]

So far, limited scholarly research and regulatory efforts have been made in the field of data protection to classify dark patterns. Attempts to categorise these deceptive practices within the context of data protection are scarce,[36] and regulatory authorities across EU Member States (MS) have been slow to establish official taxonomies.[37] Currently, the taxonomy closest to an official categorisation is that of the EDPB, which focuses on deceptive design patterns in social media interfaces.[38] This taxonomy provides a comprehensive, albeit non-exhaustive, overview of dark patterns commonly found on online platforms based on the GDPR. The Guidelines do not reference the DSA because their publication predates the Act's introduction and entry into force. Although initially

[33] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 11.

[34] This is the case for the 2022 European Commission (EC) study, which sought to categorise all dark patterns based on two axes: the component of the choice architecture that the practice affects and the component of the consumer decision-making process that the practice targets in order to encourage a change in behaviour.

European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022).

[35] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 11.

[36] From an academic and legal research perspective, noteworthy authors are Bosch and others and Luiza Jarovsky.

For more information, consult Christoph Bosch, 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' (2016) 4 Proceedings on Privacy Enhancing Technologies 237 and Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN.

[37] Of note, the Norwegian Consumer Agency (Forbrukerrådet) published its own categorisation of dark patterns based on an analysis of how prominent digital services implement malicious designs and nudge users toward privacy-invasive actions. See Forbrukerradet, *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (2018). The French National Commission on Informatics (CNIL) published a report which focuses, among other things, on deceptive designs and their effect on the privacy of data subjects based on the GDPR principles. See CNIL, *Shaping Choices in the Digital World - From dark patterns to data protection: the influence of ux/ui design on user empowerment* (IP Reports, Innovation and Foresight N06, CNIL 2019).

[38] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns'.

intended for *social media* platforms, the EDPB and scholars have clarified that the categories and types of dark patterns are not to be interpreted restrictively and can be applied to various online interfaces.[39] Therefore, this thesis will rely on the EDPB taxonomy, as it provides a consistent framework for analysing dark patterns across different online platforms while aligning with EU data protection standards.

2.2.2 EDPB Guidelines on Deceptive Design Patterns

The Guidelines introduce six categories of dark patterns, each of them containing several types of deceptive design patterns.

The first category, *Overloading*, refers to deceptive design patterns which overwhelm users with mass requests, information, options, or possibilities, in an attempt to stop them from going further and force them to consent to certain data practices, often prompting them to share more data or unintentionally allow data processing against their expectations.[40] One of the approaches in this category is *continuous prompting*, where users are persistently requested data or authorisations for new uses of their personal data. The constant interruptions can lead to user fatigue, causing them to relent and provide more personal information or accept data uses they might otherwise reject.[41] Another method is the *privacy maze*, which hinders users' access to specific information or controls related to exercising their data protection rights by requiring them to navigate numerous pages.[42] This complexity, coupled with the lack of a clear, comprehensive overview, discourages users from taking necessary actions. Additionally, the *too many options* method overwhelms users, leading to

[39] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 11.

See also Camilla Serraiotto, Francesca Tugnoli and Eleonora Auletta, 'Dark patterns in the online marketing economy' (*ICTLC*, 2023) <www.ictlc.com/dark-patterns-in-the-online-marketing-economy/?lang=en> accessed 30 August 2024; and Laura Liguori, 'Ediscom Case: The Garante Sanctioned The Use Of Dark Patterns For The First Time' (*Mondaq*, 2023) <www.mondaq.com/italy/privacy-protection/1317668/ediscom-case-the-garante-sanctioned-the-use-of-dark-patterns-for-the-first-time> accessed 30 August 2024.

[40] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 3, 10, and 65.

[41] ibid, 65.

[42] ibid, 65.

decision paralysis or accidental oversight of critical settings related to their data protection preferences or rights.[43]

The second category, *Skipping*, refers to the UI or journey being designed in such a way that users overlook or forget about all or some of the data protection aspects.[44] A notable approach here is *deceptive snugness*, where the most privacy-invasive features are enabled by default. This exploits the tendency of users to stick with pre-selected options, resulting in a lower likelihood of users changing these defaults, even when given the opportunity.[45] Another method, *look over there*, places irrelevant or distracting elements in competition with important data protection actions or information. As users follow these distractions, they may lose focus on the data protection measures they originally intended to address.[46]

The third category, *Stirring*, influences user choices by appealing to their emotions or through visual cues that nudge them toward specific decisions.[47] *Emotional steering* is a common method in this category, where emotionally charged language or visual elements, such as colours or images, are used to frame information in a way that evokes positive or negative emotions. This manipulation can lead users to make decisions that may not align with their best interests.[48] Similarly, the *Hidden in plain sight* method employs specific visual styles to subtly encourage users to select less privacy-protective options, downplaying the visibility of more privacy-conscious choices.[49]

Fourth, *Hindering* or *Obstructing* is another category where users are deliberately made to struggle or find it nearly impossible to access information or manage their data effectively.[50] One such approach is *Dead End*, where users searching for controls or information are met with broken or missing links,

[43] ibid, 66.

[44] ibid, 3, 10, and 66.

[45] ibid, 66.

[46] ibid, 66.

[47] ibid, 3, 10, and 67.

[48] ibid, 67.

[49] ibid, 67.

[50] ibid, 3, 10, and 68.

preventing them from completing their intended actions.[51] Another is *Longer Than Necessary*, where the user journey is deliberately extended, requiring more steps to engage data protection controls than to activate data-invasive options.[52] This design deters users from pursuing privacy-protective actions. *Misleading Action* is another approach, where users are led to perform actions they did not intend due to a discrepancy between what is expected and what is provided. This inconsistency discourages users from seeking out data protection measures. [53]

The fifth category, *Left in the dark*, involves hiding data protection information or controls, leaving users uncertain about how their data is processed or what controls they have.[54] *Conflicting Information* is a method where users are presented with contradictory information, leading to confusion and inaction, often resulting in users defaulting to pre-set, possibly invasive, settings.[55] Another method, *Ambiguous Wording or Information*, employs vague or unclear language when providing information to users, leaving them unsure of how their personal data will be used or how they can exercise control over it.[56]

Finally, the *Fickle* category describes designs that create an unstable and inconsistent interface, making it difficult for users to understand the nature of data processing, make informed choices, or locate relevant controls.[57] The *Lacking Hierarchy* design type presents data protection information in a disorganised manner, confusing users and preventing them from fully understanding or managing how their data is processed.[58] *Decontextualisation* involves placing data protection information or controls on a page that is out of context or unintuitive to look at, making it unlikely that users will find them

[51] ibid, 68.

[52] ibid, 68.

[53] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 68.

[54] ibid, 4, 10, and 70.

[55] ibid, 70.

[56] ibid, 70.

[57] ibid, 4, 10, and 69.

[58] ibid, 69.

when needed.[59] *Inconsistent Interface* refers to variations in the interface across different contexts or devices, causing users to struggle with locating necessary information or controls, leading to unintentional actions regarding their personal data.[60] *Language Discontinuity* occurs when, despite the service being offered in the official language(s) of the country where users reside, the data protection-related information is not provided in those languages. This disconnect prevents users from fully understanding how their personal data is processed or how to exercise their rights.[61]

For ease of reference, Annex 1 summarises the dark pattern categories, types, and definitions.

2.3 Dangers of Dark Patterns and their Impact on Privacy

While scholarly research has underscored the harmful effects of dark patterns on users, supporting empirical evidence is still emerging.[62] Current literature indicates that the harms stemming from interactions with deceptive patterns can be both material, such as financial loss, and non-material, including loss of autonomy, cognitive burden, and invasion of privacy. [63]

As mentioned, the use of dark patterns often compels users to disclose more personal data than intended, heightening their privacy risks. However, quantifying privacy harms caused by dark patterns is challenging due to the lack of measurable metrics.[64] Moreover, user complaints may be limited because individuals often remain unaware that their privacy has been compromised. This is due to the difficulty in recognising and assessing the harm associated with personal data transactions, especially when the immediate benefits of using a

[59] ibid, 69.

[60] ibid, 69.

[61] ibid, 70.

[62] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 21-22.

Early studies mainly focused on developing taxonomies, followed by research examining the prevalence of these deceptive designs. Recently, efforts have shifted towards empirically assessing their impact on user decision-making.

[63] Johana Gunawan and others, 'Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions' [2022] CSLAW '22: Proceedings of the 2022 Symposium on Computer Science and Law 181.

[64] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 25.

service obscure the potential long-term privacy costs.[65] There is also no consensus among experts on which practices are most harmful; some users view privacy infringements as most problematic, while others focus on other impacts.[66] Nevertheless, certain impacts on data protection, such as diminished autonomy, increased profiling risk, and the erosion of the validity of consent, are evident.

Personal autonomy refers to an individual's ability to make independent choices with genuine understanding and endorsement of those decisions.[67] Dark patterns undermine this autonomy by leading consumers to make decisions they might not otherwise choose, often creating an illusion of control rather than real agency.[68] From a rights-based perspective, dark patterns erode individual decision-making and autonomy.[69] The concept of 'decisional privacy', which protects individuals from unwanted interference in their actions and decisions, is closely tied to autonomy and is compromised when manipulation invades internal thought processes, diminishes free will or interferes with a user's self-interest.[70] For autonomy to be meaningful, individuals must have reasonable means to choose freely among options to achieve their goals, a freedom that deceptive designs directly threaten.[71]

---

[65] ibid.

See also Forbrukerradet, Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy (2018).

[66] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 39.

[67] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 23.

See also Harry Brignull, 'Part 1: Diving into the world of deception', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[68] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 23.

[69] ibid, 92.

[70] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 92.

[71] Tim Kollmer, 'Digital Sludging in the Privacy Context: Evidence of a Multigroup Analysis' (2022) 4 AMCIS 2022

Furthermore, the scale of data collection in online environments gives platform providers unprecedented insights into consumer vulnerabilities, far surpassing what is possible offline.[72] This insight, combined with UIs designed to manipulate choice architecture, significantly increases the risks associated with these practices.[73] The resulting extensive personal data collection and excessive user tracking enable the creation of detailed consumer profiles, identifying preferences, habits, and cognitive biases.[74] Such profiling can be exploited against users' interests, exposing them to risks of data misuse, thereby undermining their data protection rights.[75] Some designers may employ data-driven practices, known as hyper-nudging, to create highly personalised choice environments, tailoring nudges to individual profiles.[76] This large-scale data collection threatens not only privacy but also the integrity of individual decision-making. Hyper-nudging compromises autonomy by violating both 'informational privacy', which pertains to the ability to control who has access to one's personal data and to what extent, and decisional privacy.[77] This practice undermines users' ability to control their personal information and make uninfluenced decisions, raising significant concerns about the ethical implications of such data-driven manipulation techniques in online environments.

Additionally, the evolution of more effective deceptive design practices raises concerns about the effectiveness, or lack thereof, of the expression of

---

Proceedings <https://aisel.aisnet.org/amcis2022/sig_hci/sig_hci/4/> accessed 30 August 2024.

[72] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 40.

[73] ibid, 20.

[74] Szymon Osmola, 'Neither Rules nor Standards: How to Regulate Dark Patterns' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4515963> accessed 30 August 2024, 10.

See also Sebastian Rieger and Caroline Sinders, 'Dark Patterns: Regulating Digital Design' [2020] Stiftung Neue Verantwortung, 18.

[75] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 21.

[76] Marjolein Lansing, '"Strongly Recommended" Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies' (2019) 32 Philosophy & Technology 549 <https://doi.org/10.1007/s13347-018-0316-4> accessed 30 August 2024.

[77] ibid.

consent, which is paramount to privacy self-management.[78] The implementation of dark patterns severely undermines the value of data subjects' consent to personal data processing, as their behaviour is swayed through environmental cues and interface design that exploit heuristics and social norms. Consequently, individuals are often unable to provide meaningful and informed consent to the processing of their personal data.[79]

The issues discussed above only begin to reveal the full impact of dark patterns on data protection and privacy rights. Although further empirical research is necessary, the current analysis already reveals substantial concerns that threaten core aspects of data protection. The following chapters will explore the aforementioned issues from a regulatory perspective, focusing on problems such as transparency requirements, the validity of consent, and data protection by Design (DPbD), with a focus on the legal frameworks designed to address dark patterns from a data protection perspective.

[78]Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' (2015) 1880 Harvard Law Review <https://ssrn.com/abstract=2171018> accessed 30 August 2024.

[79] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 21.

3. The General Data Protection Regulation and Dark Patterns

3.1 Introduction to the GDPR

Over two decades ago, the European Community recognised the need to harmonise data protection standards across its MS to facilitate cross-border data transfers within the EU, which led to the adoption of the Data Protection Directive[80] (DPD).[81] However, as an EU directive, the DPD required transposition into national laws, resulting in inconsistent implementation across MS. This inconsistency led to varying levels of data protection, where certain data processing activities were lawful in one MS but potentially unlawful in another, undermining the Directive's objective to harmonise data protection standards and hindering the free flow of data within the internal market.[82] To address these shortcomings, the GDPR was adopted in 2016 to replace the DPD. Unlike directives, regulations apply directly in all MS, offering greater legal certainty and removing potential obstacles to the free flow of personal data within the EU.[83] The GDPR has a dual purpose: to update and strengthen the DPD, but also to adopt a technology-neutral approach,[84] making it as future-proof as possible by focusing on principles rather than specific rules tied to particular types of processing or technologies.

The GDPR sets out rules to safeguard the protection of personal data, applying to all data processing by controllers and processors within the EU and those outside the EU that offer services to or monitor individuals within the EU. The GDPR outlines comprehensive rules governing personal data processing, encompassing principles and defining lawful processing grounds. It also grants individuals a range of rights and requires high levels of transparency.

---

[80] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ L281/31.

[81] Paul Voigt and Axel von dem Bussche, 'Introduction and 'Checklist'', *The EU General Data Protection Regulation (GDPR)* (Springer, Cham 2017) <https://doi.org/10.1007/978-3-319-57959-7_1> accessed 30 August 2024, 1 and 2.

[82] Paul Voigt and Axel von dem Bussche, 'Introduction and 'Checklist'', *The EU General Data Protection Regulation (GDPR)* (Springer, Cham 2017) 2.

[83] ibid, 3.

[84] General Data Protection Regulation, Recital 15.

Although the GDPR does not explicitly mention dark patterns, it is crucial in regulating deceptive designs from a data protection perspective within the EU, as it applies to dark patterns where they entail the processing of personal data.[85] However, these practices typically emerge during the data collection phase, embedded in the design interface, rather than during data processing itself.[86] Dark patterns can lead to incompliance with data protection laws and may infringe upon the principles and specific provisions of the GDPR. [87]

The following sections will discuss key GDPR provisions[88] relevant to regulating dark patterns in the EU, alongside significant CJEU cases that, although not explicitly focused on dark patterns, are crucial to this issue. Additionally, connections between these GDPR provisions, case law, and the EDPB taxonomy of dark patterns will be explored. For ease of reference, Annex 2 provides an overview of how EDPB-defined dark patterns intersect with the GDPR.

3.2 Applicable GDPR Provisions to Dark Patterns

3.2.1 GDPR Principles – Fairness as a starting point

As a foundational reference, Article 5 GDPR outlines the data protection principles applicable to the compliance of online interfaces.[89] The principle of fairness[90] is crucial in assessing whether deceptive design patterns exist on an online platform. Despite its importance, the GDPR provides little concrete guidance on the application and enforcement of fairness, often associating it

[85] Inge Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4411537> accessed 30 August 2024, 8.

See also General Data Protection Regulation, Article 2.

[86] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN.

[87] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 75.

[88] The Recitals, albeit non-binding, provide an important interpretative value to the Regulation and will therefore also be considered.

[89] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 11.

[90] General Data Protection Regulation, Article 5(1)(a).

with transparency and lawfulness without fully clarifying its meaning.[91] The EDPB describes fairness as an overarching principle, requiring that personal data is not processed in ways that are unjustifiably detrimental, unlawfully discriminatory, unexpected, or misleading to the data subject.[92] Therefore, where an interface lacks accurate information or displays misleading design patterns, it may constitute unfair processing, as the CJEU ruled in *Orange Romania*.[93]

From a philosophical standpoint, fairness in data processing could be defined as handling personal data in a manner that: (a) honours the reasonable expectations of data subjects; (b) avoids causing them harm; (c) refrains from deceptive data collection; and (d) considers the broader implications for individual and collective interests.[94] According to this perspective, dark patterns violate the fairness principle by disregarding these expectations, negatively affecting decision-making, exploiting cognitive biases during data collection, and undermining privacy rights.[95] Therefore, the fairness principle is an overarching

[91] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 45.

[92] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0, 2020) 17.

[93] Case C-61/19 Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) [2020] ECLI:EU:C:2020:901.

§48-49 provide a relevant framework for addressing dark patterns as unfair processing under data protection law. The court emphasizes two key points: the necessity of providing detailed, specific information to data subjects, and the importance of avoiding misleading contractual terms that could confuse users about their ability to refuse consent. These principles directly apply to user interfaces employing dark patterns. The court's focus on the "informed nature of consent" suggests that interfaces lacking proper information or using deceptive design tactics may be engaging in unfair processing. The ruling thus offers a legal basis for challenging dark patterns, indicating that practices which obscure information or mislead users about their choices could violate data protection law. It strengthens the argument that transparent, clear, and non-manipulative interface design is essential for ensuring fair data processing and valid user consent.

[94] Information Commissioner's Office, 'Principle (a): Lawfulness, fairness and transparency' (*Information Commissioner's Office (ICO)*) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/> accessed 30 August 2024.

[95] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 44.

standard, with any use of deceptive design patterns being non-compliant, regardless of adherence to other data protection principles.[96]

3.2.2 Transparency

The GDPR mandates that any personal data processing be transparent to data subjects, ensuring they are fully informed when their data is collected, used, consulted, or otherwise processed.[97] Articles 5(1)(a) and 12(1) GDPR require online platform providers to present relevant information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[98] Recital 39 GDPR further extends this transparency requirement beyond mere data protection notices and data subject rights, encompassing all information and communication pertaining to data processing. Furthermore, data subjects must be informed about the risks, rules, safeguards, and rights associated with the processing of personal data, including how to exercise those rights.[99]

The importance of these transparency obligations was emphasised in *WhatsApp Ireland,*[100] where the Irish Data Protection Commission (DPC),[101] supported by the EDPB,[102] found that WhatsApp infringed the GDPR. The case highlighted that spreading information across multiple documents, failing to provide sufficiently granular information on the legal bases for processing, and inadequately explaining data transfers constitute a breach of transparency

[96] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 11.

[97] General Data Protection Regulation, Recital 39.

[98] General Data Protection Regulation, Articles 5(1)(a) and 12(1).

[99] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 12.

[100] Case T-709/21 WhatsApp Ireland Ltd v European Data Protection Board [2022] ECLI:EU:T:2022:783.

[101] Irish Data Protection Commissioner, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, IN-18-12-2 (2022).

[102] European Data Protection Board, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (2021).

See also Case T-709/21 WhatsApp Ireland Ltd v European Data Protection Board [2022] ECLI:EU:T:2022:783.

obligations.[103] Similarly, dark patterns often obfuscate key information and mislead users about how their data is processed, directly contravening the transparency and fairness principles.

As illustrated in Annex 2, nearly all dark patterns defined by the EDPB violate the fairness and transparency principles. These standards are designed to ensure that users understand how their personal data is processed and how they can exercise control over it.[104]

3.2.3 Purpose Limitation and Data Minimisation

The GDPR requires personal data processing to have specific, explicit, and legitimate purposes, as per Article 5(1)(b) GDPR. Practices that coerce users into providing more data than necessary, particularly during the sign-up phase and at any stage of the user account's life cycle – such as through frequent, repetitive consent requests or misleading prompts (*continuous prompting*) – contradict the purpose limitation principle.[105]

The data minimisation principle, intrinsically linked to purpose limitation, requires that data processing be adequate, relevant, and limited to what is necessary.[106] Dark patterns that deceive users into sharing excessive information, such as by using deceptive customisation options or pre-selecting data-sharing settings (*deceptive snugness*), contravene this principle. Techniques like emotional manipulation or complex activation processes (*emotional steering*) exacerbate the risk of unnecessary data collection,

---

[103] The resulting €225 million fine demonstrates the seriousness with which regulators view such violations, setting a precedent that could be applied to challenge deceptive design practices, including dark patterns, in digital environments.

[104] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 76.

[105] Examples include misleading users about the true purpose of data collection, like disguising telemarketing as two-factor authentication or failing to clarify that subscribing to a newsletter is a condition for accessing content.

CNIL, Shaping Choices in the Digital World - From dark patterns to data protection: the influence of UX/UI design on user empowerment (IP Reports, Innovation and Foresight N06, CNIL 2019).

[106] General Data Protection Regulation, Article 5(1)(c).

See also Inge Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' [2023] SSRN, 8.

highlighting how dark patterns frequently lead to data processing that exceeds the original purposes.[107]

3.2.4 Lawfulness of Processing and Consent

The GDPR's primary influence in regulating dark patterns is in safeguarding data subjects' consent for personal data processing. Consent is essential, as it legitimises processing based on the data subject's ability to make informed decisions.[108] Dark patterns undermine this by manipulating decision-making, preventing individuals from providing genuine, informed consent. While other legal bases for processing do not require affirmative actions from data subjects, the GDPR mandates that consent must be given through a clear, affirmative action, reflecting a freely given, specific, informed, and unambiguous agreement.[109]

Consent obtained through dark patterns cannot be deemed valid as it fails to reflect true free choice. Therefore, if dark patterns can be shown to negatively impact the decision-making process of an individual, any consent given under their influence cannot be considered genuine and reflective of free choice, as the elements manipulated by the controller are not within the awareness of the individuals.[110] The GDPR also explicitly states that pre-ticked boxes or inactivity do not constitute valid consent, as the CJEU upheld in *Planet 49*.[111] Consent

[107] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 77.

[108] General Data Protection Regulation, Article 6(1)(a).

See also Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 34.

[109] General Data Protection Regulation, Recital 32.

[110] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 35.

[111] Case C-673/1 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH [2019] ECLI:EU:C:2019:246.

The Court ruled that consent must be given by a clear affirmative act, where requiring users to untick a box to opt out of processing is not sufficient. It was also emphasised that inaction is insufficient to establish whether consent is a freely given and informed decision. A direct link can be drawn with *deceptive snugness* as defined by the EDPB, as the most data-invasive feature was enabled by default, and it could be reasonably expected that data subjects would not untick the box.

must be specific to each processing purpose, and any system that prevents users from providing separate consent for each activity or makes its withdrawal difficult is non-compliant.[112]

Additionally, consent must be revocable at any time, and data subjects must be informed of this right.[113] If consent cannot be easily withdrawn without adverse effects, or if the choice is not genuinely free, then it cannot be considered as freely given,[114] as affirmed by the CJEU in *Orange Romania.*[115] The cognitive disparity between controllers and data subjects is significant: controllers and interface designers have the technical expertise to influence the decision-making of individuals in a specific direction, while data subjects often lack awareness of cognitive biases and the manipulation techniques used by service providers.[116] This disparity underscores the need for stringent consent practices.

The EDPB highlights that practices falling under the *overloading*, *skipping*, *stirring*, *hindering*, and *left in the dark* categories constitute dark patterns which infringe Articles 4(11) and 7 GDPR on how consent should be obtained.[117]

---

[112] General Data Protection Regulation, Recital 43.

[113] General Data Protection Regulation, Article 7(3).

[114] General Data Protection Regulation, Recital 42.

[115] Case C-61/19 Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) [2020] ECLI:EU:C:2020:901.

See also §52: The CJEU ruled that a telecommunications contract clause stating the customer consented to ID copy collection and storage does not constitute valid consent where (i) the consent box was pre-ticked by the provider; (ii) the contract terms are capable of misleading customers about their ability to refuse consent; and (iii) the provider unduly influences the customer's freedom to object by requiring an additional form to refuse consent. This case can be adapted to the current definition of dark patterns: pre-ticked boxes can be likened to *deceptive snugness*, while the contracts' misleading terms can be associated with *misleading action* practices, and imposing the requirement of filling in a form in order to opt-out of the processing amounts to *longer than necessary* dark patterns, which refer to user journeys designed to make privacy-enhancing choices more cumbersome for data subjects compared to data-invasive options.

[116] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 35.

[117] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 78.

3.2.5 Automated Decision-Making

The GDPR does not explicitly prohibit personalised commercial practices, permitting them if data processing adheres to its rules. However, it could be contended that personalised advertising might be considered an automated decision under Article 22 GDPR, which grants individuals the right not to be subject to decisions made entirely through automated processing (including profiling) that have legal or similarly significant effects.[118]

The recent CJEU judgment in *Schufa*[119] broadens the interpretation of 'automated decision', potentially extending to personalised advertising practices that rely on automated profiling. The key issues relate to whether personalisation practices are solely automated and whether they have legal or similarly significant effects on consumers. This determination is case-specific, considering factors such as the intrusiveness of profiling, tracking across platforms, and the exploitation of vulnerabilities. The Article 29 Working Party suggests that targeted advertising often does not produce 'similarly significant effects' unless specific circumstances warrant it.[120] However, the *Schufa* ruling's emphasis on the cumulative effect of processing activities could support a broader application of Article 22 GDPR to certain personalised advertising practices. Specific circumstances to consider include the intrusiveness of profiling, tracking across platforms, individuals' expectations, advertising delivery methods, and exploitation of vulnerabilities. The *Schufa* interpretation potentially strengthens protection against manipulative practices in digital advertising, particularly those involving dark patterns or exploiting contextual and permanent vulnerabilities. Such practices could be regarded as having a 'similarly significant effect', warranting the application of Article 22 GDPR unless the data subject provides explicit consent to the processing.[121]

---

[118] General Data Protection Regulation, Article 22(1).

[119] Joined Cases C-26/22 and C-64/22 *UF and AB v Land Hessen* [2023] ECLI:EU:C:2023:958.

[120] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01, 2018).

[121] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 79.

3.2.6 Privacy by Design and by Default

The principles and obligations above are reinforced by Article 25(1) GDPR, which requires controllers to implement appropriate technical and organisational measures that uphold data protection principles. Furthermore, Article 25(2) GDPR stipulates that these measures must ensure that only necessary personal data is processed by default.[122] The EDPB underscores that integrating DPbD into UI design is a crucial approach to avoid dark patterns from the outset. Effective strategies to prevent dark patterns are encapsulated in the fundamental components of implementing data protection by default (DPbDf), and include ensuring user autonomy, clear communication of rights, processing data in alignment with user expectations, maintaining a power balance, absence of deception, and providing accurate information about data processing.[123] User interfaces should inherently comply with GDPR, whereas deceptive designs, such as *deceptive snugness*, *longer than necessary*, and *dead-end,* contradict the DPbD and DPbDf principles.[124]

The above aligns with the responsibilities set on controllers, who must demonstrate compliance with GDPR principles as outlined in Article 5(1) GDPR.[125] Consequently, the accountability principle should be made evident in UI design, ensuring that the design and user journey document users' acknowledgement of data protection information, their voluntary consent, and their ability to easily exercise their rights.[126]

---

[122] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 13.

[123] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) 77.

See also European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0, 2020)

[124] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 13.

[125] General Data Protection Regulation, Article 5(2) and 24.

[126] European Data Protection Board, 'Guidelines 03/2022 on deceptive design patterns', 12.

3.3 Application of the GDPR to Dark Patterns in Practice

Aside from relevant CJEU rulings mentioned in previous sections, national Data Protection Authorities (DPAs) have increasingly started to address organisations using dark patterns, often through GDPR enforcement. Over the past five years, nearly a hundred cases have been addressed by DPAs, with many addressing GDPR violations linked to dark patterns, even if not explicitly initiated on those grounds.[127] Noteworthy cases which were specifically addressing dark patterns include the Italian Garante fining a digital marketing company €300,000 for using misleading graphic interfaces,[128] and the Irish DPC imposing a €405 million fine on TikTok for using deceptive patterns targeting children.[129]

---

[127] Deceptive Patterns, 'Legal cases' (*Deceptive Patterns*) <www.deceptive.design/cases?jurisdiction=EU+&+UK> accessed 30 August 2024.

[128] Garante per la Protezione dei Dati Personali, Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A. (9870014, 2023).

Ediscom S.p.A. was fined for using misleading graphic interfaces in its campaigns. When users were asked for marketing consent and left the consent boxes unchecked, a pop-up with a prominent "consent" button appeared, while a less visible "continue without accepting" option was placed at the bottom of the page. The Garante ruled that this design constituted dark patterns aimed at manipulating users into giving consent, citing EDPB Guidelines.

See also Kristof Van Quathem and Laura Somaini, 'Italian Garante Fines Digital Marketing Company Over Use of Dark Patterns' (*Italian Garante Fines Digital Marketing Company Over Use of Dark Patterns*, 2023) <www.insideprivacy.com/eu-data-protection/italian-garante-fines-digital-marketing-company-over-use-of-dark-patterns/> accessed 30 August 2024.

[129] Irish Data Protection Commission, *Irish Data Protection Commission announces €345 million fine of TikTok* (ICO 2023) <www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok> accessed 30 August 2024.

See also European Data Protection Board, Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR (2022).

The EDPB and the DPC found that Instagram infringed the GDPR in two key ways regarding child users: (i) Meta processed contact information from children's business accounts without a legal basis, and (ii) Instagram set child user accounts to "public" by default, exposing their content to anyone. Additionally, the EDPB reviewed TikTok's design practices and found that its pop-ups for children aged 13-17 were biased, pushing users towards less privacy-protective options. The Registration Pop-Up defaulted to "Skip," promoting public accounts, while the Video Posting Pop-Up highlighted "Post Now" over "Cancel," making it harder to choose private settings. These practices were deemed unfair under the GDPR, leading the DPC to impose a €405 million fine on Meta and order TikTok to address these deceptive practices.

4. The Digital Services Act and Dark Patterns

4.1 Introduction to the DSA

While online platforms - such as search engines, social media, and e-commerce sites – are becoming increasingly integral to our social and economic lives, the existing EU regulations governing digital services had, until recently, remained largely unchanged since the e-Commerce Directive[130] was adopted in 2000. In December 2020, the European Commission (EC) introduced the Digital Services Act Package,[131] including two draft laws: the DSA and the Digital Markets Act.[132] These new measures aim to create a more equitable landscape and increase online platforms' accountability for the content they host. The DSA seeks to foster a transparent and secure online environment by defining the responsibilities and obligations of various stakeholders, thereby reshaping the rights and duties of digital service providers, online users, customers, and businesses within the EU.[133]

Despite its name, the DSA does not govern all digital services but is limited to 'intermediary services', which are any service involving the transmission and storage of user-generated content. These include 'mere conduit services'[134] such as internet access providers and messaging apps,

[130] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1.

[131] European Commission, 'The Digital Services Act package' (*Shaping Europe's Digital Future*) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 30 August 2024.

[132] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L265/1.

[133] European Parliament: European Parliamentary Research Service, *Briefing: Digital Services Act* (2022).

[134] *Mere conduit service*: service consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.

See Digital Services Act, Articles 3(g)(i) and 4.

'caching services'[135] like content delivery networks, and 'hosting services'[136] including social networks, content-sharing services, discussion forums, and cloud services.

Notwithstanding its scope, the DSA holds significant practical importance, affecting activities like watching videos, cloud storage, reading reviews, social media use, and internet access. These services are crucial not only for economic purposes but also for social, recreational, cultural, and political reasons, which underscores the DSA's relevance in addressing the evolving impact of digital intermediaries on society.[137]

4.2 Scope and Structure of the DSA

The DSA's primary goal is to establish a safe, predictable, and innovation-conductive online environment that effectively upholds the fundamental rights enshrined in the Charter of Fundamental Rights of the EU.[138] The DSA applies without prejudice to other Union laws regulating the provision of information society services within the internal market, including the legislative framework applicable to the protection of personal data in the EU – that is, the GDPR.[139]

As abovementioned, the DSA's material scope applies to intermediary services operating within the EU Single Market, focusing on the *services* rather than the *providers*. Consequently, a provider offering multiple services may

---

[135] *Caching service*: service consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request.

See Digital Services Act, Articles 3(g)(ii) and 5.

[136] *Hosting service*: service consisting of the storage of information provided by, and at the request of, a recipient of the service.

See Digital Services Act, Articles 3(g)(iii) and 6.

[137] Folkert Wilman, 'The Digital Services Act (DSA) - An Overview' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4304586> accessed 30 August 2024, 1.

Recent events have highlighted the key role of these services, particularly hosting services and social media platforms, in organising uprisings, conducting elections, managing public health crises, and shaping public discourse around major events like inter-state conflicts.

[138] Charter of Fundamental Rights of the European Union [2012] OJ C26/391.

Also, Digital Services Act, Article 1(1).

[139] Digital Services Act, Recital 10.

have some that fall under the DSA and others that do not. The provider's place of establishment is irrelevant; rather, the DSA's applicability depends on whether the service is offered to users within the EU.[140]

The DSA introduces a tiered regulatory approach, with the rules becoming stricter at each successive level based on the role, size, and impact of a given online player within the digital ecosystem. Rather than distinguishing by service *type*, the DSA categorises services by their *size*, determined by the number of monthly active users.[141] The layered structure of obligations can be visualised as a four-tiered pyramid, with each level regulating different services. The base level sets fundamental obligations for *intermediary services*, meaning that all services must observe them. The next set of obligations only applies to *hosting services*, such as those that involve storing user-provided information. The third level introduces stricter obligations for *online platforms* such as online marketplaces, app stores, collaborative economy platforms, and social media platforms, which are subsets of hosting services characterised by storing users' data and disseminating it to the public.[142] At the pyramid's peak are *Very Large Online Platforms* (VLOPs) and *Very Large Online Search Engines* (VLOSEs), which are services that serve over 45 million monthly users in the EU, corresponding to roughly 10% of the EU population.[143]

The EC designates VLOPs and VLOSEs based on user numbers reported by the platforms and search engines, and these services must comply with the DSA within four months of designation.[144] The designation triggers specific rules addressing the unique risks posed by these large services to EU citizens and society, including issues related to illegal content, fundamental rights, public

[140] Digital Services Act, Article 2(1).

[141] Folkert Wilman, 'The Digital Services Act (DSA) - An Overview' [2023] SSRN, 3.

[142] Digital Services Act, Article 3(i).

[143] Digital Services Act, Recital 76 and Article 33.

[144] Digital Services Act, Article 34.

See also European Commission, 'DSA: Very large online platforms and search engines' (*Shaping Europe's digital future*) <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops> accessed 30 August 2024.

security, and well-being. To date, about 25 services have been designated as VLOPs[145] and two as VLOSEs.[146]

The obligations set by the DSA are cumulative, meaning that if a service falls under multiple categories, it must adhere to all relevant obligations. For instance, a VLOP/VLOSE will have to adhere to rules applicable to intermediary services, hosting services, and online platforms, in addition to the specific requirements for VLOPs/VLOSEs. Conversely, *mere conduit services,* like internet access providers, are only bound by the basic obligations outlined at the lowest layer of the pyramid.[147]

Annex 3 introduces a visual representation of the aforementioned layered structure and its corresponding obligations.

4.3 Applicable DSA Provisions to Dark Patterns

4.3.1 Main DSA Provisions

In February 2024, the DSA became directly applicable across the EU, marking a milestone as it explicitly addresses dark patterns in legislation for the first time. Indeed, Article 25(1) DSA prohibits online platforms from designing, organising, or operating their interfaces in ways that "deceive or manipulate the recipients of their service or otherwise materially distorts or impairs their ability to make free and informed decisions".[148]

Although the term *dark pattern* is not explicitly mentioned in Article 25 DSA itself, the accompanying Recital 67 clarifies that the prohibition includes

[145] Very Large Online Platforms designated by the European Commission as of July 2024: AliExpress, Amazon Store, Apple Store, Pornhub, Booking.com, Google Play, Google Maps, Google Shopping, YouTube, Shein, Linkedin, Facebook, Instagram, XNXX, Pinterest, Snapchat, Stripchat, TikTok, X (formerly Twitter), Temu, XVideos, Wikipedia, and Zalando.

European Commission, 'Supervision of the designated very large online platforms and search engines under DSA' (*Shaping Europe's digital future*) <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> accessed 30 August 2024.

[146] Very Large Online Search Engines designated by the European Commission as of July 2024: Google Search and Bing.

See European Commission, 'Supervision of the designated very large online platforms and search engines under DSA' (*Shaping Europe's digital future*).

[147] Folkert Wilman, 'The Digital Services Act (DSA) - An Overview' [2023] SSRN, 4.

[148] Digital Services Act, Article 25(1).

them. It defines dark patterns as "*practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. 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*".[149] It also emphasises that providers should refrain from deceiving or nudging users, and from distorting or impairing their autonomy, decision-making, or choices through the structure, design, or functionalities of online interfaces.[150] The DSA, like the GDPR, prioritises individual autonomy by explicitly protecting the ability of users to make free, informed, and autonomous decisions.[151] This focus on autonomy aligns with foundational research, which highlights autonomy as central to the functioning of dark patterns. The DSA emphasises autonomy in its provisions and recitals, using terms like "unwanted behaviours", "undesired decisions", and "negative consequences"[152] as well as "distorts or impairs the ability to make free and informed decisions".[153]

The DSA provides limited detail on how dark patterns manifest in practice. Article 25(3) DSA identifies three types: (i) giving undue prominence to certain choices when seeking a user's decision; (ii) repeatedly requesting the user's choices, particularly through pop-ups that disrupt user experience; and (iii) complicating the process of terminating a service compared to subscribing.[154] The provision also empowers the Commission to issue additional guidelines, suggesting that further clarification and guidance on the prohibition of dark patterns may be anticipated in the future.

---

[149] Digital Services Act, Recital 67.

[150] Digital Services Act, Recital 67.

The Recital further elaborates on a non-exhaustive list of practices considered as dark patterns, which are outlined in Annex 4.

[151] M Leiser and Cristiana Santos, 'Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface' (2024) 15(1) BILETA Special Issue <https://ssrn.com/abstract=4431048> accessed 30 August 2024, 21.

[152] Digital Services Act, Recital 67.

[153] Digital Services Act, Article 25.

See also Cristiana Santos and others, 'Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA?' [2024] SSRN, 6.

[154] Digital Services Act, Article 25(3).

Importantly, the DSA's prohibition on dark patterns applies only to *online platforms* and *VLOPs/VLOSEs*.[155] These categories primarily encompass services offered by tech giants, which, due to their size and influence, present far greater societal risks than smaller platforms. Consequently, large platforms and search engines must meet the highest due diligence standards, with obligations proportional to their societal impact, as their extensive user base can lead to significant systemic risks across the EU. To prevent imposing disproportionate burdens, micro and small enterprises, as well as intermediary and hosting services, are exempt from this prohibition unless their user base qualifies them as a VLOP or VLOSE.[156]

Article 25(2) DSA exempts practices already covered by the GDPR,[157] raising concerns about the DSA's effectiveness in addressing dark patterns. Since most dark patterns fall under the GDPR or other legislation like the UCPD, this exception may limit the DSA's impact. While the GDPR governs personal data-related dark patterns and the UCPD addresses business-to-consumers transactions, certain dark patterns – e.g., infinite scroll, autoplay, and nagging – may still evade regulation, particularly in business-to-business contexts. Moreover, the DSA's ability to address more advanced dark patterns, like those in the metaverse or next-generation interfaces such as hyper-nudges and human-robot manipulation, remains unclear, suggesting that the Act may not fully capture emerging manipulative practices.[158]

Since this thesis uses the EDPB's dark pattern taxonomy, Annex 4 offers an overview of the dark pattern types identified in the DSA and their alignment with the EDPB taxonomy.

---

[155] These are the two highest tiers set by the DSA.

The exception to the prohibition is outlined in the Digital Services Act, Article 19.

[156] Digital Services Act, Article 19.

[157] The DSA holds a complimentary role to the GDPR in regulating dark patterns, as is outlined by Article 25(2) and Recital 67: "[rules preventing dark patterns] should be interpreted as covering prohibited practiced falling within the scope of the [DSA] to the extent that those practices are not already covered under the [GDPR]".

[158] Cristiana Santos and others, 'Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA?' [2024] SSRN <http://dx.doi.org/10.2139/ssrn.4899559> accessed 30 August 2024, 21.

4.3.2 Other Applicable Provisions

The DSA includes significant measures for risk assessments, audits, and risk mitigation, which are pivotal for combatting deceptive practices. These requirements, similarly to the prohibition on dark patterns, apply exclusively to VLOPs and VLOSEs.

Annual risk assessments are mandatory for VLOPs/VLOSEs to identify potential DSA violations. These assessments require platforms to closely examine their products based on the DSA rules, document areas of risk, retain all related records, and ensure they are accessible to authorities. This process shifts some investigative responsibilities from regulators to businesses.[159] Although these assessments do not explicitly target dark patterns, the DSA's prohibition on deceptive practices compels service providers to critically detect, examine, document, and mitigate potential manipulative design elements within their platforms.[160]

Additionally, VLOPs and VLOSEs must engage independent external auditors to assess compliance with the DSA. These audits are expected to be more objective and thorough than internal assessments.[161] Providers are required to cooperate, granting auditors access to internal data, and must develop an implementation plan to address any identified issues. The audit reports, which will be submitted to authorities and made publicly available, underscore the crucial role of independent auditors in detecting and combating deceptive practices.[162] While these audits are not explicitly targeted at dark patterns, they will inevitably encompass them, offering recommendations for their elimination.

---

[159] Digital Services Act, Article 34.

See also Harry Brignull, 'Chapter 30: Changes afoot in the European Union', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[160] Harry Brignull, 'Chapter 30: Changes afoot in the European Union', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[161] Digital Services Act, Article 42.

[162] Digital Services Act, Article 37.

See also Harry Brignull, 'Chapter 30: Changes afoot in the European Union', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

4.4 Application of the DSA to Dark Patterns in Practice

The DSA introduces a new role, the 'Digital Services Coordinator' (DSC), which each MS must appoint. DSCs oversee all DSA-related matters within their respective countries. While enforcement can be handled at national level, the EC retains the authority to intervene, especially if enforcement by a MS is deemed too lenient and potentially undermines the DSA's objectives. This mechanism ensures consistent application of the DSA across the EU and discourages MS from adopting lax enforcement, including in areas such as dark patterns, aiming to attract VLOPs and VLOSEs to establish their headquarters locally.[163]

Considering the DSA's relative novelty, there have been very few cases before the CJEU yet. Thus far, the Court has addressed cases involving VLOPs/VLOSEs disputing their designation by the EC, and issues related to profiling-based recommender systems, but has yet to rule on dark patterns under the DSA.[164]

The DSA centralises the enforcement of the obligations set upon VLOPs and VLOSEs at the EU level, thereby leaving it in the hands of the EC.[165] Over the past year, the EC initiated formal proceedings against several online platforms, enabling it to take further enforcement steps such as imposing interim measures and non-compliance decisions.[166] Noteworthy formal proceedings relating to the prohibition of dark patterns are those initiated

[163] Digital Services Act, Article 49.

See also Harry Brignull, 'Chapter 30: Changes afoot in the European Union', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[164] Case C-639/23 P(R) *European Commission v Amazon Services Europe* Sàrl [2024] ECLI:EU:C:2024:277.

Also see, for example, Case T-139/24 R *WebGroup Czech Republic, a.s. v European Commission* [2024] ECLI:EU:T:2024:475.

[165] Digital Services Act, Articles 65-74.

See also Gabriela Zanfir-Fortuna and Vasileios Reviles, 'EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR' (*Future of Privacy Forum*, 2023) <https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/> accessed 30 August 2024.

[166] Digital Services Act, Articles 65-74.

against Meta,[167] and those initiated against X.[168] While the Commission has yet to reach a conclusion on Meta, it has preliminarily determined that X is in breach of Article 25 DSA. Its assessment highlights concerns about X's 'verified accounts' system, which allegedly deceives users and fails to align with industry standards, thereby impairing users' ability to make informed decisions.[169] If these preliminary findings are upheld, X could face fines of up to 6% of its global annual turnover, corrective measures, and potentially enhanced supervision and penalty payments to ensure compliance.[170]

[167] European Commission, 'Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act' (*Press release*, 30 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373> accessed 30 August 2024.

[168] European Commission, 'Commission opens formal proceedings against X under the Digital Services Act' (*Press release*, 18 December 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 30 August 2024.

[169] European Commission, 'Commission sends preliminary findings to X for breach of the Digital Services Act' (*Press release*, 12 June 2024) <https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3761> accessed 30 August 2024.

[170] ibid.

5. Analysis of the Legal Framework applicable to Dark Patterns

The effectiveness of any legislative framework inherently depends on legal certainty, and the regulation of dark patterns is no exception. The interplay between the DSA and existing laws, such as the GDPR, might challenge and, at times, limit legal certainty, mostly due to the sometimes-confusing approach as to whether action against a given dark pattern should be taken based on one or the other regulation.[171]

This chapter will examine how the GDPR and DSA address dark patterns to protect data protection rights in the EU. It will explore the interplay between the GDPR and DSA, the legal terminology used in both regulations and the enforcement of dark pattern prohibitions. Based on this analysis, potential solutions and improvements will be proposed.

Of note, some sections may briefly reference the UCPD, as it, alongside the GDPR, takes precedence over aspects covered by the DSA.[172]

5.1 Interplay between the GDPR and the DSA

5.1.1 Effectiveness and Limitations

Although the DSA and the GDPR serve distinct purposes, both aim to protect fundamental rights in a data-driven society and strengthen the European Single Market. The DSA establishes rules for digital services, emphasising safeguards against individual and systemic harms online, and introduces a novel transparency and accountability framework for digital platforms. As digital services inherently involve data processing, including personal data, the GDPR ensures that such processing respects individuals' fundamental rights while promoting the free movement of personal data within the EU.[173] Both play crucial roles in protecting users from manipulative design practices that may lead to privacy violations. The GDPR, although not explicitly mentioning dark patterns, provides principles around consent, transparency, and data protection

[171] Tom Akhurst and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo - Chair Digital, Governance and Sovereignty <www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/09/Dark-Patterns.pdf> accessed 30 August 2024, 15.

[172] Digital Services Act, Article 2(4).

[173] Gabriela Zanfir-Fortuna and Vasileios Reviles, 'EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR' (*Future of Privacy Forum*, 2023).

by design that can be applied to regulate their use. The DSA, on the other hand, directly prohibits dark patterns, defining them as practices that impede users from making autonomous and informed choices.[174]

The two regulations create a complex regulatory environment for digital service providers due to their overlapping scopes. The broad definitions of 'controllers' and 'processing of personal data' under the GDPR mean that intermediaries regulated by the DSA may also be considered controllers.[175] This overlap necessitates compliance with both regulations, with the GDPR generally taking precedence over aspects of the DSA.[176]

When examining the technical design of online platforms, the DSA and the GDPR set broad standards regarding the technical aspects of interface design rather than prohibiting specific practices.[177] Article 25 GDPR on DPbD and DPbDf requires controllers to integrate data protection into the design of their systems, ensuring that appropriate technical and organisational measures are implemented to ensure the protection of data subject rights. Conversely, Article 25 DSA is presented as a prohibition rather than a principle by addressing the implementation of manipulative online interface designs directly. As such, the GDPR focuses on preventing manipulation related to *data collection*, while the DSA covers broader aspects of manipulative *design*, making the two regulations complementary in regulating dark patterns.[178]

A key distinction between the dark pattern definitions discussed in Chapter 1 and those in the DSA is that the latter specifies that deceptive patterns do not need to be intentional.[179] This implies a lower threshold for triggering the DSA, requiring only that dark patterns affect individuals without

---

[174] Dan Cooper and others, 'The EU Stance on Dark Patterns' (*Covington*, 2023) <www.insideprivacy.com/eu-data-protection/the-eu-stance-on-dark-patterns/> accessed 30 August 2024.

[175] Gabriela Zanfir-Fortuna and Vasileios Reviles, 'EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR' (*Future of Privacy Forum*, 2023).

[176] Digital Services Act, Recitals 10 and 67, and Article 25(2).

[177] Tom Akhurst and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo - Chair Digital, Governance and Sovereignty, 16.

[178] ibid, 16.

[179] Digital Services Act, Recital 67 refers to "practices that materially distort or impair, either *on purpose or in effect".*

needing to prove intent.[180] By focusing on user impact rather than platform intent, this approach broadens the Act's scope, potentially capturing a wider range of problematic designs, including those that unintentionally manipulate users. This aligns with the DSA's objective of fostering a safer online environment. Moreover, the DSA's risk assessment, audit, and mitigation measures for higher-tier services could play a crucial role in identifying and disclosing deceptive practices. However, the stringent obligations regarding deceptive designs apply only to VLOPs and VLOSEs, exempting micro and small-sized enterprises. This exemption could allow smaller businesses to evade stricter requirements and continue using deceptive tactics with minimal repercussions, highlighting a challenge for regulators in enforcing consistent oversight across all platforms.[181] This contrasts with the GDPR's broader scope, which covers all organisations processing personal data, ensuring that even small online platforms are subject to the rules applicable to dark patterns.

The interplay between the DSA and the GDPR regarding dark patterns has a key limitation: although their respective scopes may appear to be generally clear, potential overlap exists when an entity is both a controller under the GDPR and an online platform under the DSA. Some scholars raised concerns that the theoretical framing of the DSA's interrelationship with the GDPR does not fully resolve the practical overlap between these provisions.[182] Specifically, the literature lacks consensus on which *specific* dark pattern practices fall under the DSA. Indeed, Article 25(2) DSA explicitly excludes practices already covered by the GDPR, which creates ambiguity in determining whether a dark pattern practice violates 'only' one or both pieces of legislation.[183] Consequently, the parallel application of these laws in the digital sector could lead to jurisdictional issues among national DPAs and DSCs, necessitating closer cooperation

[180] Harry Brignull, 'Chapter 30: Changes afoot in the European Union', *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023).

[181] ibid.

[182] Natali Helberger and others, 'Digital Fairness for Consumers' [2024] BEUC - European Consumer Organisation.

[183] Cristiana Santos and others, 'Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA?' [2024] SSRN, 1.

between these bodies to ensure effective enforcement and consistency in regulatory actions.[184]

5.1.2 Recommendations

In 2014, the EDPS cautioned that despite privacy and data protection being fundamental rights and public interests recognised in the Treaties, the lack of coordination between consumer protection and data protection policies could weaken both the enforcement of competition rules and the development of privacy-enhancing services.[185] Although discussions about adopting a more integrated and collaborative approach have continued, the understanding of how these policies interplay and their incorporation into digital platform regulations remains underdeveloped.[186] The preceding section underscores that while the DSA and GDPR are intended to be complementary in tackling dark patterns, their practical alignment may be challenging. To address this, it is essential that the Commission, which is authorised to issue guidelines on the DSA's dark pattern prohibition, develops these guidelines in close collaboration with national DPAs and the EDPB, especially considering the GDPR's primary role in protecting against manipulative design. This cooperation is essential to ensure alignment, coherence, and consistency between the two regulations, thereby upholding legal certainty.[187] However, this approach would still rely on soft law measures, raising concerns among scholars about the extent of their effectiveness in regulating deceptive designs.[188]

---

[184] Iga Małobęcka-Szwast, '"Dark patterns" targeted by EU institutions' (*Lexology*, 2023) <www.lexology.com/library/detail.aspx?g=cee82fe8-25c4-445d-9eaa-c747d1f0cc64> accessed 30 August 2024.

[185] European Data Protection Supervisor, Preliminary Opinion of the European Data Protection Supervisor - Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy (EDPS 2014) 37.

[186] Wolfgang Kerber, 'Taming Tech Giants: The Neglected Interplay between Competition Law and Data Protection (Privacy) Law' (2022) 67(2) Antitrust Bulletin <http://dx.doi.org/10.2139/ssrn.4045528> accessed 30 August 2024, 3.

[187] Gabriela Zanfir-Fortuna and Vasileios Reviles, 'EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR' (*Future of Privacy Forum*, 2023).

[188] Szymon Osmola, 'Neither Rules nor Standards: How to Regulate Dark Patterns' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4515963> accessed 30 August 2024, 41.

Adapting the EU framework, particularly the GDPR, to address dark patterns could prove beneficial in the long term. Although historically, the law has avoided closely regulating design to prevent stifling innovation, dark patterns can undermine existing protections for individuals and erode trust in service providers.[189]

To address this, a future revision of the GDPR could refine consent requirements and reformulate the fairness principle to encompass manipulative designs and cognitive biases.[190] Currently, the GDPR does not directly address cognitive biases, manipulative design, or interference in decision-making. It also fails to fully explore the fairness principle[191], nor addresses how unfair design practices can impact data protection. Recognising and mitigating cognitive biases is essential when managing data subjects' consent, especially given the significant processing power of technology companies that amplifies the inherent asymmetry in the online environment.[192] As previously noted, although the GDPR offers extensive protection during the data processing phase, it remains largely silent on the pre-processing phase, where dark patterns frequently arise, leaving individuals exposed to potential exploitation. Therefore, interface design practices must reflect data protection principles, ensuring that they mitigate, rather than exacerbate, the imbalance between data subjects and controllers.[193]

Furthermore, a future update of the DSA's prohibition on dark patterns should expand its scope to include all entities falling under the Act, rather than focusing on specific players. The current limitation may undermine consumer

[189] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 2.

[190] ibid, 3.

See also Agnieszka Kitkowska, 'The Hows and Whys of Dark Patterns: Categorizations and Privacy' in Nina Gerber, Alina Stöver and Karola Marky (eds), *Human Factors in Privacy Research* (Springer, Cham 2023) 193.

[191] Of note, although the GDPR introduces and refers to the notion of "fairness" on numerous occasions in its text, it does not actually define it anywhere.

[192] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 50.

[193] ibid, 50.

protection and could distort the market.[194] A universal application of the prohibition would better address emerging trends and technologies that exploit users' privacy through manipulative designs, ensuring that *all* service providers maintain high standards of fairness, transparency, and data protection. This approach could also reduce regulatory fragmentation, offering a unified framework to protect users from manipulative practices across all types of services.

5.2 Legal definitions

5.2.1 Effectiveness and Limitations

Since the GDPR's terminology does not directly address dark patterns, this section will primarily focus on the legal terms introduced by the DSA. Although the latter aims to eliminate dark patterns through prohibition, implementing this ban may prove challenging due to its abstract wording.[195] Indeed, several terms in Article 25 DSA lack definitional certainty, which introduces various risks and complications.

First, the DSA's definition of prohibited '*design, organisation, or operation* of online interface' is vague and potentially includes aspects of online architecture not traditionally associated with dark patterns. Current approaches to dark patterns primarily focus on observable interface features, which critics argue overlooks emerging manipulative practices through interface personalisation.[196] This has led to calls for a broader understanding of 'manipulative practices', suggesting a shift from 'dark patterns' to more comprehensive concepts like "manipulative online choice architectures" to encompass dynamic practices like behavioural algorithms.[197] Although Article 25 and Recital 67 DSA do not explicitly refer to emerging dynamic practices, their broad wording could encompass them. The prohibited examples in Article 25 align with the traditional, static definition of dark patterns, but the absence of

[194] Victoria de Posson, 'Dark Patterns: Protecting consumers without hindering innovation' (*European Tech Alliance*, 2023) <https://eutechalliance.eu/dark-patterns-protecting-consumers-without-hindering-innovation/> accessed 30 August 2024.

[195] Folkert Wilman, 'The Digital Services Act (DSA) - An Overview' [2023] SSRN, 10.

[196] Tom Akhurst and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo - Chair Digital, Governance and Sovereignty, 12.

[197] ibid, 12.

the term 'dark patterns' and the use of broader phrases like "online interface and design" raise questions about its intent. Specifically, the phrase "online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates" and the reference to the "structure, design or functionalities of an online interface"[198] could plausibly be understood as encompassing dynamic dark patterns based on personalisation, especially given the Article's goal to address gaps in dark pattern regulation. The prohibition covers not only design and functionalities but also operations that deceive or manipulate. Although the DSA's emphasis on manipulation and autonomy highlights these issues' significance, many questions about the scope and application of these provisions remain unanswered.[199]

Second, it is not clear whether the DSA's prohibition on dark patterns extends to *potential* deceit in addition to *actual* deceit. Traditionally, potential deception has sufficed, as noted in the EC's Guidelines, which reference the UCPD's standard that a pattern need only be *likely* to deceive, not that it actually did.[200] Since both the DSA and UCPD aim to eliminate dark patterns, they could be interpreted similarly, suggesting that the DSA might also prohibit both actual and potential deception. This interpretation would align with the UCPD's requirement that a practice must *likely cause* a user to make a decision they would not have otherwise made.[201]

Third, Article 25 DSA does not specify the *recipient* standard for determining whether a pattern is likely to deceive users – that is, from an 'average consumer' or 'vulnerable consumer' perspective. While a complementary approach with other EU regulations, like the UCPD, could employ the 'average consumer' standard except when targeting vulnerable groups, the DSA may need a different approach due to the digital asymmetry between platforms and users. Some scholars contend that all digital consumers

[198] In Recital 67 DSA.

[199] Tom Akhurst and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo - Chair Digital, Governance and Sovereignty, 12-13.

[200] European Commission, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021, OJ C526/1) 31.

[201] Tom Akhurst and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo - Chair Digital, Governance and Sovereignty, 14.

are inherently vulnerable, given platforms' access to detailed user profiles and control over the user environment.[202] This allows for the exploitation of consumer vulnerabilities, blurring the distinction between average and vulnerable consumers and making all users potentially susceptible to manipulation. Lowering the recipient standard below the 'average consumer' benchmark could ease the burden of proof for demonstrating illegal dark patterns, aligning with the DSA's goal to address information asymmetries. However, critics caution against relaxing standards, as it may blur the distinction between legitimate persuasion and manipulation.[203]

Finally, the DSA lacks criteria to quantify the *magnitude* and *thresholds* of dark patterns, or the *harms* they cause. It also does not account for the varying degrees and combinations of pattern categories that platforms may use. Similarly, the GDPR does not specify the level of harm necessary to trigger enforcement. This gap might require the EDPB, the Commission, or another regulator to establish guidelines that provide a scale of severity for these harms.[204]

In conclusion, although the DSA attempts to tackle dark patterns, it does so through vague standards, deferring key decisions to other institutions and relying on soft law measures, whose effectiveness remains uncertain.[205]

5.2.2 Recommendations

Clarifying the legal terms introduced by the DSA regarding the prohibition of dark patterns is essential, and guidance from the Commission would influence how these prohibitions are interpreted and enforced.

---

[202] Weiwei Yi and Zihao Li, 'Mapping the Scholarship of Dark Pattern Regulation: A Systematic Review of Concepts, Regulatory Paradigms, and Solutions from an Interdisciplinary Perspective' [2024] CREATe Centre <https://arxiv.org/pdf/2407.10340> accessed 30 August 2024, 19.

[203] Tom Akhurst and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo - Chair Digital, Governance and Sovereignty, 14-15.

[204] Johana Gunawan and others, 'Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions' [2022] CSLAW 22: Proceedings of the 2022 Symposium on Computer Science and Law 181, 186.

[205] Szymon Osmola, 'Neither Rules nor Standards: How to Regulate Dark Patterns' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4515963> accessed 30 August 2024, 43.

To address the challenges identified, establishing clear criteria could be effective.[206] These could involve applying absolute and relative thresholds based on different normative perspectives to evaluate whether a practice meets the criteria for a dark pattern.[207] These thresholds could incorporate legal definitions of deceptiveness or empirical metrics comparing the practice's impact against a "baseline" UI.[208]

Protection is determined by each legal framework's scope rather than the harm's nature: the GDPR addresses practices involving personal data and fair processing, while the DSA targets online platforms. However, harm from dark patterns often extends beyond these boundaries.[209] Given the absence of established criteria to quantify and assess the magnitude of dark patterns and their associated harm, it is essential for regulators to develop guidelines that provide a framework for evaluating their severity.[210]

---

[206] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 16.

[207] Aranesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3 Proceedings of the ACM on Human-Computer Interaction 1.

Mathur and others classify existing research on dark patterns into two types of choice architecture: (1) modifying the decision space, with attributes like asymmetry, restriction, disparate treatment, and covert tactics, and (2) manipulating the information flow, with attributes such as deception and information hiding. They argue for the importance of addressing dark patterns based on normative principles such as collective and individual welfare, regulatory goals, and autonomy. They suggest that to evaluate the "darkness" of deceptive designs, one should analyse them through these normative lenses and tailor studies to consider who might be affected – whether the general public or specific user groups.

See also Agnieszka Kitkowska, 'The Hows and Whys of Dark Patterns: Categorizations and Privacy' in Nina Gerber, Alina Stöver and Karola Marky (eds), *Human Factors in Privacy Research* (Springer, Cham 2023) 192.

[208] Aranesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3 Proceedings of the ACM on Human-Computer Interaction 1.

See also OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 16.

[209] Inge Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' [2023] SSRN, 18.

[210] Johana Gunawan and others, 'Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions' [2022] CSLAW '22: Proceedings of the 2022 Symposium on Computer Science and Law 181, 186.

Scholarly research suggests several approaches to quantify and define harm caused by dark patterns. For instance, measuring the level of effort required from users to avoid privacy-intrusive dark patterns could help gauge the magnitude of its harm.[211] Alternatively, a typology of privacy harms – encompassing reputational, emotional, discriminatory, informed choice, and autonomy harm – could offer a more nuanced understanding of dark patterns' impact.[212] Additionally, shifting the burden of proof over platform providers to demonstrate that no harm was caused by dark patterns could further strengthen effective enforcement.[213]

It is crucial to recognise that hastily formalising dark patterns in law and policy threatens to dilute the concept. Should the threshold for categorisation be too low, an "if everything is a dark pattern, then nothing is a dark pattern" paradox may arise.[214] This challenge reflects the difficulty of aligning digital market realities with established legal frameworks. The legal discourse on dark patterns, particularly in the privacy domain, remains underdeveloped, lacking a consolidated definition, classification, and clear criteria for identifying such practices. This ambiguity complicates the task of determining which practices violate the GDPR or the DSA.[215] The debate around dark patterns centres on

[211] Johana Gunawan and others, 'Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions' [2022] CSLAW '22: Proceedings of the 2022 Symposium on Computer Science and Law 181.

See also OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 25.

[212]Danielle Citron and Daniel Solove, 'Privacy Harms' (2021) 102(793) Boston University Law Review <www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf> accessed 30 August 2024.

See also OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 25.

[213] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 41.

See also European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022).

[214] Catalina Goanta and Cristiana Santos, 'Dark Patterns Everything: An Update on a Regulatory Global Movement' [2023] Network Law Review <www.networklawreview.org/digiconsumers-two/> accessed 30 August 2024.

[215] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN, 36.

balancing individual harm, user autonomy, and consumer protection while also addressing digital asymmetry between companies and consumers. Greater harmonisation of definitions and taxonomies is necessary to effectively address these tensions, considering factors such as consumer autonomy, digital literacy, and the broader role of regulatory requirements across legal systems.[216] Crucially, one must question whether providing more details is always beneficial in digital environments, and explore normative questions concerning the ideal role of online platform providers and data subjects within this framework. Addressing these issues could develop a more nuanced understanding of dark patterns, avoiding over-categorisation whilst maintaining the concept's utility in protecting users and fostering fair digital practices.[217]

5.3 Enforcement and Harmonisation of the Dark Pattern Prohibition

5.3.1 Effectiveness and Limitations

As this paper has demonstrated, one approach to addressing dark patterns is through legislation and regulation. However, fragmented enforcement could undermine their effectiveness. Specifically, enforcing dark pattern prohibitions under both the GDPR and the DSA presents challenges due to overlapping scopes and differing enforcement mechanisms.

Firstly, while the DSA explicitly prohibits dark patterns, it defers to the GDPR for issues involving personal data. This overlap creates ambiguity, making it difficult to determine which regulation takes precedence in specific situations, potentially leading to jurisdictional conflicts between DPAs and DSCs.[218]

Secondly, the GDPR and DSA's enforcement structures differ significantly. The GDPR's enforcement is primarily national, with cross-border cases coordinated through the EDPB's One-Stop-Shop mechanism. Conversely, the DSA centralises enforcement for VLOPs and VLOSEs at the EU level, overseen by the Commission, while leaving enforcement for other intermediary services

[216] ibid, 36.

[217] Catalina Goanta and Cristiana Santos, 'Dark Patterns Everything: An Update on a Regulatory Global Movement' [2023] Network Law Review.

[218] Iga Małobęcka-Szwast, '"Dark patterns" targeted by EU institutions' (*Lexology*, 2023).

As a reminder, 'DPAs' refers to Data Protection Authorities while 'DSCs' mean Digital Services Coordinators.

to national DSCs.[219] However, the inconsistent approach in designating national authorities, combined with varying interpretations and enforcement of rules by MS, poses challenges for effective enforcement. Therefore, the same dark pattern may be regulated under either the GDPR or DSA, depending on the authority involved, leading to uneven application of the law across jurisdictions. This disparity in enforcement may depend on the resources available to each authority and their relative power.[220] This ambiguity not only complicates enforcement but also creates uncertainty for market participants, as businesses may struggle to plan their operations and understand their responsibilities if it is unclear which laws apply, who enforces them, and how to comply with them.[221]

The interplay between the DSA and GDPR underscores the need for consistent interpretation and application of the law. However, the DSA's enforcement and supervision frameworks do not formally recognise the need for cooperation between DSCs and DPAs, or the EDPB and the European Board for Digital Services (EBDS). Despite the lack of formal cooperation mechanisms, it is essential to establish collaborative processes within their respective competencies to ensure effective enforcement. As the DSA is implemented, the complexity of its interaction with the GDPR will likely become more apparent, emphasising the necessity for such cooperation.[222]

5.3.2 Recommendations

Given the current limitations in policymaking, regulation, and enforcement regarding dark patterns, shifting some responsibilities to other market actors, such as service providers and users, could be a potential solution. These measures should be complementary to robust regulatory and enforcement efforts, rather than as standalone solutions.

---

[219] Gabriela Zanfir-Fortuna and Vasileios Reviles, 'EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR' (*Future of Privacy Forum*, 2023).

[220] Tom Akhurst and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo - Chair Digital, Governance and Sovereignty, 20.

[221] ibid, 20.

[222] Gabriela Zanfir-Fortuna and Vasileios Reviles, 'EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR' (*Future of Privacy Forum*, 2023).

Raising awareness and educating individuals through authority-led information campaigns can mitigate the adverse effects of dark patterns.[223] Educational interventions that enhance consumers' cognitive skills and ability to manage their online environment can be effective.[224] For instance, encouraging procedural rules before making choices and initiatives to improve "manipulation literacy" or "critical digital literacy" can empower consumers to avoid deceptive practices.[225] Additionally, browser tools and apps designed to detect, reduce, or remove dark patterns can further aid in protecting privacy.[226] Equally important are service providers' efforts in self-regulation. Organisations should embed principles related to online advertising, UI design, and commercial practices into their core operations.[227] Illustratively, committing to Corporate Digital Responsibility can prompt businesses to take on greater digital responsibilities beyond legal requirements.[228] Crucially, service providers must first understand what dark patterns are, making initial guidance and education essential.

Another approach to address dark patterns is expanding the DSA's existing tools. The DSA introduces 'trusted flaggers'[229] – experts designated by DSCs to identify and report potentially illegal content – and a whistleblower

---

[223] Agnieszka Kitkowska, 'The Hows and Whys of Dark Patterns: Categorizations and Privacy' in Nina Gerber, Alina Stöver and Karola Marky (eds), *Human Factors in Privacy Research* (Springer, Cham 2023) 194.

[224] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 46.

[225] ibid, 46.

[226] For example, Mathur and others suggest a browser extension that automatically detects dark patterns, while the Dark Pattern Detection Project is working on an AI-based app to recognise and redesign dark patterns for users.

OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 47; Aranesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3 Proceedings of the ACM on Human-Computer Interaction 1.; DAPDE, 'Dark Pattern Detection Project' <https://dapde.de/en/> accessed 30 August 2024.

[227] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 48.

[228] Benjamin Mueller, 'Corporate Digital Responsibility' [2022] Springer <https://d-nb.info/1268101435/34> accessed 30 August 2024.

[229] Digital Services Act, Article 22.

European Commission, 'Trusted flaggers under the Digital Services Act (DSA)' (*Shaping Europe's digital future*, 2024) <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa> accessed 30 August 2024.

tool[230] for VLOPS and VLOSES' employees to report harmful practices. However, these mechanisms do not currently encompass the reporting of dark patterns. To enhance their effectiveness, the role of trusted flaggers should be expanded to include the reporting of dark patterns or a new category of flaggers specialising in dark patterns could be introduced.[231] Additionally, the whistleblower tool should be broadened to enable reporting of dark patterns and be made accessible to all stakeholders, including data subjects, potentially through a tip line similar to those found in other jurisdictions.[232] Improving these mechanisms could improve the identification and management of dark patterns, complementing regulatory efforts and fostering accountability in online environments.

While industry efforts, education, awareness-raising, and technical tools are valuable in protecting consumers from dark patterns and helping shape effective policies, they must be complemented by robust regulatory and enforcement measures.[233] With the substantive rules on dark patterns largely established, the focus now needs to shift toward effective enforcement amidst a fragmented regulatory landscape. Integrated enforcement approaches are essential, with existing coordination networks such as the EDPB and the EBDS facilitating cooperation at EU and national levels. The challenge lies in creating cohesion across these bodies and their respective legal domains. At a minimum, there must be joint priority-setting to clarify responsibilities and optimise

[230] European Commission, 'DSA whistleblower tool' (*Shaping Europe's digital future*, 2024) <https://digital-strategy.ec.europa.eu/en/policies/dsa-whistleblower-tool> accessed 30 August 2024.

[231] As far as the author is aware, this suggestion has not yet been introduced or is supported by other experts or scholars. The idea stems from reading about "Taskforce" groups under the GDPR, which have focused on various topics in the past.

[232] The 'Dark Pattern Tip Line' is a US website where individuals can report dark patterns they encounter online. This initiative helps researchers understand how technology exploits users by gathering examples of manipulative or unfair designs. Submissions are used for research and to inform the public, media, and policymakers, with each example reviewed before being added to the repository to illustrate individual cases from specific companies.

See Stanford Digital Civil Society Lab, 'Dark Patterns Tip Line' (*Dark Patterns Tip Line*, 2024) <https://darkpatternstipline.org/> accessed 30 August 2024.

[233] OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) 49.

resource allocation.[234] This approach would help avoid under-enforcement, resource duplication, and jurisdictional conflicts.[235] The CJEU supports this through *Meta Platforms v Bundeskartelllamt,*[236] emphasising the importance of consultation and sincere cooperation between supervisory authorities across different sectors, ensuring that decisions align while respecting their respective powers and safeguarding the objectives of relevant regulations.[237] Further integration could involve joint policymaking to clarify the interaction of legal rules, and pursuing joint cases, drawing inspiration from international collaborations like those between the International Consumer Protection and Enforcement Network and the Global Privacy Enforcement Network.[238] Adopting these collaborative models would enhance enforcement and leverage the benefits of the fragmented regulatory framework by sharing responsibilities and cooperating more effectively in combating dark patterns.

[234] For instance, data protection authorities could focus on e-commerce or social proof dark patterns, while consumer authorities might address social media or obstruction dark patterns.

[235] Inge Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' [2023] SSRN, 20.

[236] Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537.

[237] The CJEU held that it is within the power of a competition authority to recognise personal data as both an asset that is relevant to competition and as abusive conduct when it comes to violations of consumers' data protection. Importantly, this approach emphasizes cooperation between competition and data protection authorities, which is most important when regulating dark patterns across both domains. In other words, although this case was not specifically focused on dark patterns, it strengthens the legal framework for addressing manipulative design practices that infringe on data protection rights, especially when employed by dominant platforms in digital markets.

[238] A notable example is ICPEN's intervention, which led Google to require app providers to disclose data practices on the Google Play Store, a move endorsed by GPEN.

6. Conclusion

This thesis examined the complex issue of dark patterns in digital environments from a regulatory and data protection perspective within the EU. As outlined, dark patterns pose significant challenges to data protection and consumer autonomy. Both the GDPR and the DSA seek to address these issues, but their overlapping scope and varying focuses complicate enforcement and effectiveness.

The DSA marks a crucial development by explicitly banning dark patterns for the first time in EU law, yet its effectiveness is constrained by several factors. It excludes practices already covered by the GDPR, relies on vague definitions, and lacks clear criteria for distinguishing between illegal and legitimate practices or between actual and potential deceit. Furthermore, the DSA's dependence on future EC guidelines, which may address *specific* dark patterns without offering comprehensive coverage, limits its impact. Consequently, the DSA's prohibition falls short of fully addressing all manipulative practices.

Although the GDPR does not explicitly address dark patterns, its technology-neutral stance allows it to regulate some manipulative design practices. However, this indirect approach creates inconsistencies in effectively tackling dark patterns. A more direct approach, such as revising consent requirements or expanding the fairness principle to account for manipulative designs and cognitive biases, could be beneficial. Without such revisions, the GDPR may fall short of addressing the full scope of harm caused by dark patterns.

A key challenge lies in defining *what* constitutes a dark pattern in practice and determining *when* it becomes serious enough to breach existing legislation. Although the DSA provides a theoretical framework by defining dark patterns, applying this definition in practice is challenging. Determining whether a design deceives, manipulates, or materially distorts a user's ability to make an informed decision is nearly impossible without detailed guidance, which neither regulation provides. Clarification is also needed on how legal norms interact and apply when multiple regulations are applicable. The fragmented regulatory landscape in the EU, with different regulators and overlapping jurisdictions, exacerbates this issue, potentially leading to inconsistent application of the law and risking under-enforcement. Given these challenges, it is worth questioning

whether dark patterns, if deemed harmful enough to be banned, should be regulated under a specific, unified regime rather than across various legal domains. The DSA could have served as a comprehensive framework for such regulation, but instead, the EU legislator deferred to existing frameworks like the UCPD and the GDPR.

To effectively combat dark patterns, a multifaceted approach is necessary. Enhancing awareness and education among consumers and service providers is crucial. Additionally, expanding the DSA's tools, such as introducing dedicated dark pattern flaggers and enhancing whistleblowing mechanisms, could improve detection and reporting. Ultimately, while industry efforts and educational initiatives are vital, they must be complemented by robust regulatory enforcement. Integrated enforcement strategies and better coordination between existing regulatory bodies, like the EDPB and the EBDS, are essential to ensure a consistent application of rules across jurisdictions, thereby helping to address regulatory fragmentation and enhance the overall effectiveness of efforts to combat dark patterns.

In conclusion, while the DSA and GDPR provide a foundation for regulating dark patterns, their fragmented and overlapping nature limits their effectiveness. Future CJEU decisions on the dark patterns could clarify the interplay between the GDPR and the DSA, highlighting the DSA's added value and effectiveness in addressing dark patterns beyond the GDPR’s scope. Ultimately, a more unified and targeted regulatory approach, potentially supported by future legislative revisions and soft law, remains necessary to fully address dark patterns’ risks and safeguard digital users’ privacy rights across the EU.

List of References

1. Legal Sources

1.1 Legislative and Other Legal Acts

1.1.1 European

Charter of Fundamental Rights of the European Union [2012] OJ C26/391

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L281/31

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) [2016] OJ L119/1

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1

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) [2022] OJ L277/1

1.2 Case Law

1.2.1 European

Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537

Case C-61/19 *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* [2020] ECLI:EU:C:2020:901

Case C-639/23 P(R) *European Commission v Amazon Services Europe Sàrl* [2024] ECLI:EU:C:2024:277

Case C-673/1 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] ECLI:EU:C:2019:246

Case T-139/24 R *WebGroup Czech Republic, a.s. v European Commission* [2024] ECLI:EU:T:2024:475

Case T-709/21 *WhatsApp Ireland Ltd v European Data Protection Board* [2022] ECLI:EU:T:2022:783

Joined Cases C-26/22 and C-64/22 *UF and AB v Land Hessen* [2023] ECLI:EU:C:2023:958

1.3 Other Legal or Policy Documents

Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01, 2018)

European Commission, 'Commission opens formal proceedings against X under the Digital Services Act' (*Press release*, 18 December 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 30 August 2024

CNIL, *Shaping Choices in the Digital World - From dark patterns to data protection: the influence of UX/UI design on user empowerment* (IP Reports, Innovation and Foresight N06, CNIL 2019)

European Commission, *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market* (2021, OJ C526/1)

European Commission, 'Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act' (*Press release*, 30 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373> accessed 30 August 2024

European Commission, 'DSA whistleblower tool' (*Shaping Europe's digital future*, 2024) <https://digital-strategy.ec.europa.eu/en/policies/dsa-whistleblower-tool> accessed 30 August 2024

European Commission, 'DSA: Very large online platforms and search engines' (*Shaping Europe's digital future*) <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops> accessed 30 August 2024

European Commission, 'Supervision of the designated very large online platforms and search engines under DSA' (*Shaping Europe's digital future*) <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> accessed 30 August 2024

European Commission, 'The Digital Services Act package' (*Shaping Europe's Digital Future*) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 30 August 2024

European Commission, 'Trusted flaggers under the Digital Services Act (DSA)' (*Shaping Europe's digital future*, 2024) <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa> accessed 30 August 2024

Information Commissioner's Office, 'Principle (a): Lawfulness, fairness and transparency' (*Information Commissioner's Office (ICO)*) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/> accessed 30 August 2024

Irish Data Protection Commission, *Irish Data Protection Commission announces €345 million fine of TikTok* (ICO 2023) <www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok> accessed 30 August 2024

European Commission: Directorate-General for Justice and Consumers, *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report* (Publications Office of the European Union 2022) <https://data.europa.eu/doi/10.2838/859030> accessed 30 August 2024

European Data Protection Board, *Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR* (2021)

European Data Protection Board, *Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR* (2022)

European Data Protection Board, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them* (Version 2.0, 2023)

European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (Version 2.0, 2020)

European Data Protection Supervisor, *Preliminary Opinion of the European Data Protection Supervisor - Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy* (EDPS 2014)

European Parliament: European Parliamentary Research Service, *Briefing: Digital Services Act* (2022)

Forbrukerradet, *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (2018)

Garante per la Protezione dei Dati Personali, *Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A.* (9870014, 2023)

Helberger N and and others, 'Digital Fairness for Consumers' [2024] BEUC - European Consumer Organisation

Irish Data Protection Commissioner, *Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation,* IN-18-12-2 (2022)

OECD, *Dark commercial patterns* (OECD Digital Economy Papers, No. 336, OECD Publishing 2022) <https://doi.org/10.1787/44f5e846-en> accessed 30 August 2024

2. Academic Sources

2.1 Books

Brignull H, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023)

Kahneman D, *Thinking, Fast and Slow* (Farra, Straus and Giroux 20211)

Voigt P and von dem Bussche A, 'Introduction and 'Checklist'', *The EU General Data Protection Regulation (GDPR)* (Springer, Cham 2017) <https://doi.org/10.1007/978-3-319-57959-7_1> accessed 30 August 2024

2.2 Book Chapters

Kitkowska A, 'The Hows and Whys of Dark Patterns: Categorizations and Privacy' in Nina Gerber, Alina Stöver and Karola Marky (eds), *Human Factors in Privacy Research* (Springer, Cham 2023) <https://doi.org/10.1007/978-3-031-28643-8_9> accessed 30 August 2024

2.3 Journal Articles

Akhurst T and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo – Chair Digital, Governance and Sovereignty <www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/09/Dark-Patterns.pdf> accessed 30 August 2024

Bosch C, 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' (2016) 4 Proceedings on Privacy Enhancing Technologies 237 <https://doi.org/10.1515/popets-2016-0038> accessed 30 August 2024

Brignull H and others, 'Dark Patterns: Deception vs. Honesty in UI Design' [2011] A List Apart <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/> accessed 30 August 2024

Citron D and Solove D, 'Privacy Harms' (2021) 102(793) Boston University Law Review <www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf> accessed 30 August 2024

Goanta C and Santos C, 'Dark Patterns Everything: An Update on a Regulatory Global Movement' [2023] Network Law Review <www.networklawreview.org/digiconsumers-two/> accessed 30 August 2024

Graef I, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4411537> accessed 30 August 2024

Jarovsky L, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' [2022] SSRN <http://dx.doi.org/10.2139/ssrn.4048582> accessed 30 August 2024

Johana Gunawan and others, 'Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions' [2022] CSLAW '22: Proceedings of the 2022 Symposium on Computer Science and Law 181 <https://pure.uvt.nl/ws/portalfiles/portal/65614055/gunawan_santos_kamara_2022_cslaw.pdf> accessed 30 August 2024

Kerber W, 'Taming Tech Giants: The Neglected Interplay between Competition Law and Data Protection (Privacy) Law' (2022) 67(2) Antitrust Bulletin <http://dx.doi.org/10.2139/ssrn.4045528> accessed 30 August 2024

Kollmer T and Eckhardt A, 'Dark Patterns: Conceptualization and Future Research Directions' [2023] 65 Business & Information Systems Engineering 201 <https://doi.org/10.1007/s12599-022-00783-7> accessed 30 August 2024

Kollmer T, 'Digital Sludging in the Privacy Context: Evidence of a Multigroup Analysis' (2022) 4 AMCIS 2022 Proceedings <https://aisel.aisnet.org/amcis2022/sig_hci/sig_hci/4/> accessed 30 August 2024

Lansing M, '"Strongly Recommended" Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies' (2019) 32 Philosophy & Technology 549 <https://doi.org/10.1007/s13347-018-0316-4> accessed 30 August 2024

Leiser M and Santos C, 'Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface' (2024) 15(1) BILETA Special Issue <https://ssrn.com/abstract=4431048> accessed 30 August 2024

Mathur A and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' [2019] 3 Proceedings of the ACM on Human-Computer Interaction 1 <https://arxiv.org/pdf/1907.07032.pdf> accessed 30 August 2024

Mueller B, 'Corporate Digital Responsibility' [2022] Springer <https://d-nb.info/1268101435/34> accessed 30 August 2024

Osmola S, 'Neither Rules nor Standards: How to Regulate Dark Patterns' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4515963> accessed 30 August 2024

Rieger S and Sinders C, 'Dark Patterns: Regulating Digital Design' [2020] Stiftung Neue Verantwortung

Santos C and and others, 'Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA?' [2024] SSRN <http://dx.doi.org/10.2139/ssrn.4899559> accessed 30 August 2024

Solove D, 'Privacy Self-Management and the Consent Dilemma' (2015) 1880 Harvard Law Review <https://ssrn.com/abstract=2171018> accessed 30 August 2024

Wilman F, 'The Digital Services Act (DSA) - An Overview' [2023] SSRN <http://dx.doi.org/10.2139/ssrn.4304586> accessed 30 August 2024

Yi W and Li Z, 'Mapping the Scholarship of Dark Pattern Regulation: A Systematic Review of Concepts, Regulatory Paradigms, and Solutions from an Interdisciplinary Perspective' [2024] CREATe Centre <https://arxiv.org/pdf/2407.10340> accessed 30 August 2024

2.4 Other Academic Works

Zanfir-Fortuna G and Reviles V, 'EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR' (*Future of Privacy Forum*, 2023) <https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/> accessed 30 August 2024

3. Non-Academic Sources

Aislelabs, 'Customer Paths and Retail Store Layout — Part 3 (*Aislelabs*, 2018) <www.aislelabs.com/blog/customer-paths-and-retail-store-layout-part-3> accessed 30 August 2024

Cooper D and et al, 'The EU Stance on Dark Patterns' (*Covington*, 2023) <www.insideprivacy.com/eu-data-protection/the-eu-stance-on-dark-patterns/> accessed 30 August 2024

DAPDE, 'Dark Pattern Detection Project' <https://dapde.de/en/> accessed 30 August 2024

de Posson V, 'Dark Patterns: Protecting consumers without hindering innovation' (*European Tech Alliance*, 2023) <https://eutechalliance.eu/dark-patterns-protecting-consumers-without-hindering-innovation/> accessed 30 August 2024

Liguori L, 'Ediscom Case: The Garante Sanctioned The Use Of Dark Patterns For The First Time' (*Mondaq*, 2023) <www.mondaq.com/italy/privacy-protection/1317668/ediscom-case-the-garante-sanctioned-the-use-of-dark-patterns-for-the-first-time> accessed 30 August 2024

Małobęcka-Szwast I, '"Dark patterns" targeted by EU institutions' (*Lexology*, 2023) <www.lexology.com/library/detail.aspx?g=cee82fe8-25c4-445d-9eaa-c747d1f0cc64> accessed 30 August 2024

Serraiotto C, Tugnoli F, and Auletta E, 'Dark patterns in the online marketing economy' (*ICTLC*, 2023) <www.ictlc.com/dark-patterns-in-the-online-marketing-economy/?lang=en> accessed 30 August 2024

Stanford Digital Civil Society Lab, 'Dark Patterns Tip Line' (*Dark Patterns Tip Line*, 2024) <https://darkpatternstipline.org/> accessed 30 August 2024

Van Quathem K and Somaini L, 'Italian Garante Fines Digital Marketing Company Over Use of Dark Patterns' (*Italian Garante Fines Digital Marketing Company Over Use of Dark Patterns*, 2023) <www.insideprivacy.com/eu-data-protection/italian-garante-fines-digital-marketing-company-over-use-of-dark-patterns/> accessed 30 August 2024

Annex 1: Categories and Types of Dark Patterns – Definitions – based on EDPB Guidelines on Dark Patterns

Overloading	Burying users under mass of requests, information, options or possibilities in order to deter them from going further and make them keep or accept certain data practice.	
	Continuous prompting	Persistently requesting data from users or obtaining their authorisation for new uses of their data, with the intention of pressuring them to supply more personal information than is required for processing or to accept this usage. One or more devices may be used to deliver such persistent prompts. Because it interrupts their usage of the site, users are likely to give in after growing weary of having to reject the request every time.
	Privacy maze	Making it particularly difficult for users to obtain certain information, use a specific control, or exercise a data subject right, by requiring that they navigate through many pages in order to obtain the relevant information or control, without having a comprehensive and exhaustive overview available.
	Too many options	By implementing too many options to choose from, the users are unable to make any choice or accidentally overlook some settings. This may lead them to give up or miss the settings for their data protection preferences or rights.

Skipping	Designing the interface or user journey in such a way that users forget or do not think about all or some of the data protection aspects.	
	Deceptive snugness	The most data invasive features are enabled by default. Users who rely on the default effect, which encourages people to stick with a pre-selected option, are unlikely to alter it even if given the chance.
	Look over there	An element that may or may not be relevant to data protection is placed in competition with an action or piece of information related to data protection. Users who select this distracting option are likely to lose sight of the other, even if it was their main goal.

Fickle	The design of the interface is unstable and inconsistent, making it hard for users to figure out the nature of the processing, to properly make a choice concerning their data, and to find where the different controls are.	
	Lacking hierarchy	Data protection-related information is presented in a non-hierarchical manner, with multiple appearances and formats. This repetition is likely to confuse users, leaving them unable to completely comprehend how their data is processed and how to take control of it.
	Decontextualisation	Data protection information or controls are located on a page that is out of context and unintuitive to look at in that context, making it unlikely for users to finds them

	Inconsistent interface	An interface doesn't match users' expectations or various contexts (e.g., an option, such as the data protection settings, whose location has been switched with that of another option across devices). These variations may make it difficult for users to locate the information or controls they need, or they may cause them to interact with an interface element out of habit even when doing so forces them to make unfavourable decisions about their data protection.
	Language discontinuity	While the service is offered in the official language(s) of the country where users reside, data protection-related information is not. Users are unlikely to be aware of how data are processed if they are unable to read data protection information in the language in which it is presented
	Conflicting information	Conflicting pieces of information are given to users, leaving the latter unsure of what actions they should undertake and the consequences of those. A likely result is that the users will refrain from taking any action and resort to the default settings.
	Ambiguous wording or information	Ambiguous and vague terms are used when providing information to users, leaving them unsure of how their data will be processed or how they can exercise control over their personal data.

Stirring	Affecting the choice users would make by appealing to their emotions or using visual nudges.	
	Emotional steering	Employing language or visual cues (such as design, colour, image, or others) to convey information to consumers in a way that either gives them a very positive outlook – making them feel secure, good, or rewarded – or a very negative one – making them feel guilty, afraid, or punished. Users who are emotionally influenced in this way are more likely to take actions that are detrimental to their interests in data protection.
	Hidden in plain sight	Where a specific visual style or method is applied to information and data protection controls in order to nudge users to choose less restrictive and thus more invasive options.

Left in the dark	The interface is designed in a way to hide information or controls related to data protection or to leave users unsure of how data is processed and what kind of controls they might have over it.	
	Conflicting information	Conflicting pieces of information are given to users, leaving the latter unsure of what actions they should undertake and the consequences of those. A likely result is that the users will refrain from taking any action and resort to the default settings.
	Ambiguous wording or information	Ambiguous and vague terms are used when providing information to users, leaving them unsure of how their data will be processed or how they can exercise control over their personal data.

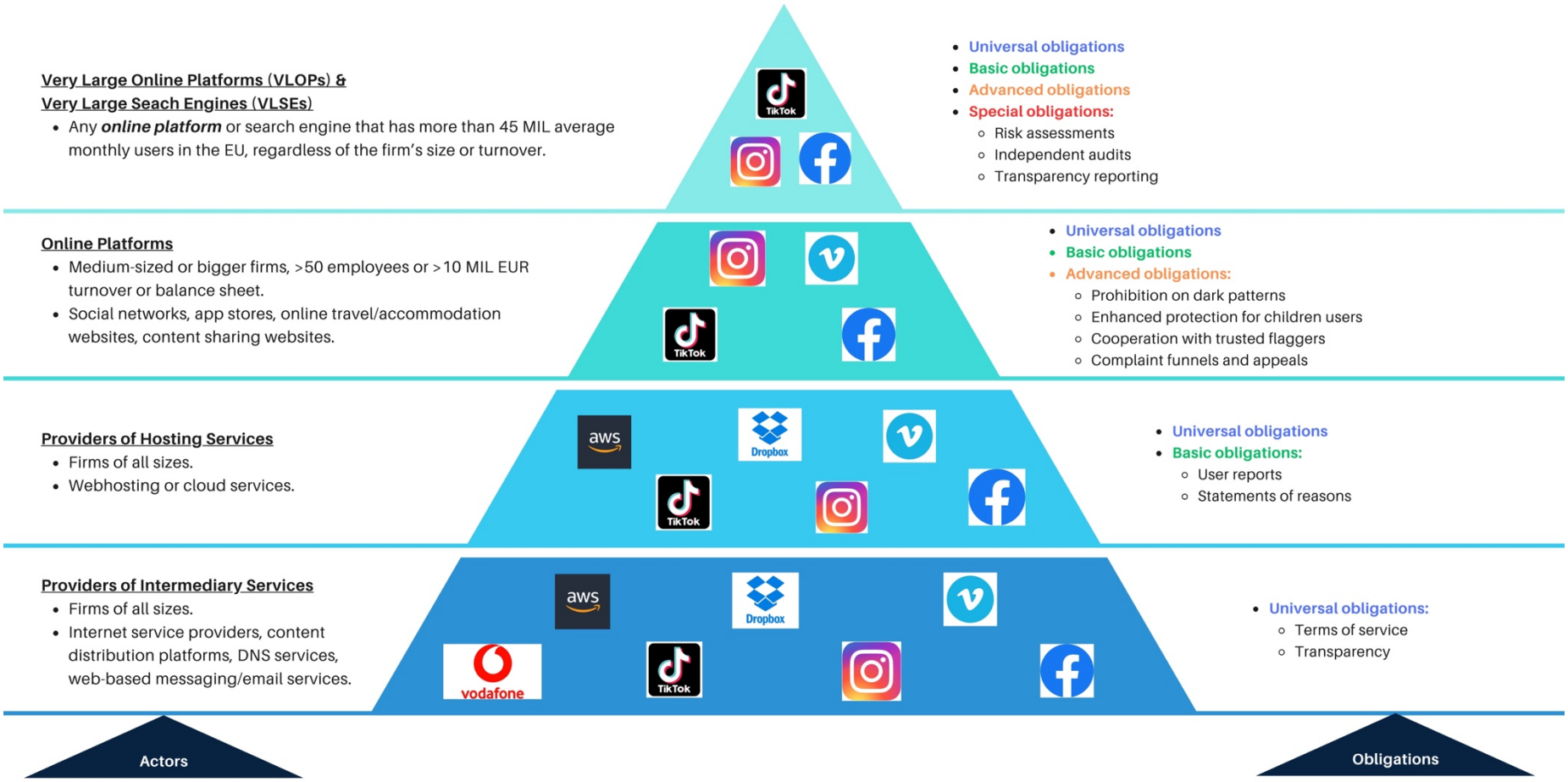
Hindering / obstructing	Hindering or blocking users in their process of obtaining information or managing their data by making the action hard or impossible to achieve.	
	Dead end	When users search for controls or information, they are unable to access it because a redirection link is either broken or unavailable, making it impossible to complete the work.
	Longer than necessary	The user journey is designed to require more steps from users when they attempt to engage a control related to data protection than when they activate data invasive options. This is likely to deter them from turning on that kind of control.
	Misleading action	Users are pushed to perform actions they did not plan to undertake when there is a discrepancy between the information and actions that are available to them. The discrepancy between users' expectations and what is provided is likely to deter them from continuing.

Annex 2: Summary of Applicable GDPR Articles to the EDPB Dark Pattern Taxonomy

		Content-based	Interface-based	Art 4(11) - Consent	Art 5(1)(a) - Transparency, Fairness	Art 5(1)(b) - Purpose Limitation	Art 5(1)(c) - Data Minimisation	Art 7- Informed consent, freely given	Art 7(2) Specific consent	Art 7(3) - Consent withdrawal	Art 8 - Children's consent	12(1) - Transparent information, easily accessible, use of clear and plain	12(2) - Easy access to rights	13 - Incomplete information	21(1) - Right to object	25(1) - Data protection by design and by default
Overloading	Continuous prompting	x	x	x	x	x		x	x							
	Privacy maze	x	x	x	x			x				x	x			
	Too many options	x			x							x				
Skipping	Deceptive snugness		x	x	x		x	x	x	x	x					x
	Look over there		x		x							x	x			
Stirring	Emotional steering	x		x	x		x	x			x	x	x			
	Hidden in plain sight		x	x	x			x				x	x			
Hindering / obstructing	Dead end	x	x		x							x	x			x
	Longer than necessary	x	x		x		x			x		x	x		x	x
	Misleading action	x		x	x				x	x		x				
Fickle	Lacking hierarchy	x			x							x	x			
	Decontextualisation		x		x							x	x			
	Inconsistent interface	x	x		x							x	x			
	Language discontinuity	x			x							x		x		

Left in the dark	Conflicting information	x		x	x				x			x				
	Ambiguous wording or information	x		x	x				x			x		x		

Annex 3: DSA Overview – Services, Types, and Obligations



Annex 4: Summary of Applicable DSA Articles and Recital to the EDPB Dark Pattern Taxonomy

This table was adapted from Cristiana Santos and others, 'Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA?' [2024] SSRN, the Digital Services Act, and the EDPB Guidelines on Dark Patterns.

Prohibited practices by Article 25(3) DSA	Prohibited practices by Recital 67 DSA	EDPB taxonomy
Article 25(3)(a) DSA: Giving more **prominence to certain choices** when asking the recipient of the service for a decision	(a) 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	**Fickle**: lacking hierarchy, decontextualisation, inconsistent interface, language discontinuity, conflicting information, ambiguous wording or information
Article 25(3)(b): **Repeatedly requesting** that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience	(b) **Repeatedly requesting** a recipient of the service to make a choice where such a choice has already been made	**Overloading**: continuous prompting, privacy maze, too many options
Article 25(3)(c): Making the procedure for terminating a service **more difficult** than subscribing to it	(c) Making the procedure of cancelling a service **significantly more cumbersome** than signing up to it (d) Making certain choices **more difficult** or time-consuming than others (e) Making it **unreasonably difficult** to discontinue purchases or to sign out from a given online platform allowing consumers to conclude distance contracts with traders	**Hindering**/**obstructing**: dead end, longer than necessary, misleading action
	(f) **Deceiving** the recipients of the service by **nudging** them into decisions on transactions	**Stirring**: emotional steering, hidden in plain sight
	(g) **Default settings** that are **very difficult** to change, and so unreasonably bias the decision making of the recipient of the service, in a way that distorts and impairs their autonomy, decision-making and choice	**Skipping**: deceptive snugness, look over there