# Towards Key Contributing Factors in Identifying Dark Pattern Autonomy Violations under the EU Digital Services Act

Sanju Ahuja
Inria Centre at Université Côte d'Azur
Valbonne, France
sanju.ahuja@inria.fr

Johanna Gunawan
Law and Tech Lab, Maastricht University
Maastricht, Netherlands
johanna.gunawan@maastrichtuniversity.nl

Nataliia Bielova
Inria Centre at Université Côte d'Azur
Valbonne, France
nataliia.bielova@inria.fr

Cristiana Teixeira Santos
School of Law, Utrecht University
Utrecht, Netherlands
c.teixeirasantos@uu.nl

## Abstract

Dark patterns refer to design practices which undermine users' ability to make autonomous and informed choices in relation to digital systems. The recent EU Digital Services Act (DSA) aims to protect users from such dark patterns and their effects. DSA Article 25 prohibits three autonomy violation types: *deception, manipulation* and *distortion/impairment*. However, for regulation of dark patterns, it is important to reason about why an observed design practice constitutes a particular autonomy violation type, to show that it indeed violates the DSA. In this work-in-progress, two experts (with HCI, CS and legal background) mapped 59 known dark patterns onto these three autonomy violation types. We then analysed our rationale for this mapping to identify eight design factors which can help determine the dark pattern autonomy violation(s). Our analysis aims to situate existing dark patterns knowledge within the DSA legal framework, to support regulation and compliance of such design practices.

## CCS Concepts

• **Human-centered computing → Empirical studies in HCI**; **Human computer interaction (HCI)**.

## Keywords

dark patterns, deceptive design, autonomy violations, Digital Services Act

**ACM Reference Format:**
Sanju Ahuja, Johanna Gunawan, Nataliia Bielova, and Cristiana Teixeira Santos. 2025. Towards Key Contributing Factors in Identifying Dark Pattern Autonomy Violations under the EU Digital Services Act. In *Designing Interactive Systems Conference (DIS '25 Companion), July 5–9, 2025, Funchal, Portugal.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3715668.3736336


*DIS '25 Companion, Funchal, Portugal*

ACM ISBN 979-8-4007-1486-3/2025/07
https://doi.org/10.1145/3715668.3736336

## 1 Introduction

Generally known as "dark patterns", [1] deceptive, manipulative, or coercive design practices are used in digital systems to increase revenue, maximize user engagement, and collect personal data. These practices impact user autonomy and influence users into making decisions they did not intend, or decisions against their best interests [1, 2, 18, 29]. Such patterns pervade web and mobile apps [9, 22], e-commerce [28, 32], social media [30, 31, 37], privacy interfaces [4, 20, 23], games [14, 41], and video streaming platforms [7]. Recently, Gray et al. [21] harmonized several taxonomies of dark patterns – five regulatory [8, 13, 15, 25, 34], four academic [4, 18, 24, 28], and one practitioner [5, 6] taxonomies – into a three-level ontology, thus uniting dark patterns and their definitions into a unified body of knowledge.

A 2022 EU Commission report [25] finds that "97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern". In the EU, the Digital Services Act (DSA) [10], which came into force on February 17, 2024, explicitly prohibits the use of dark patterns for online platforms. DSA Article 25 states that *"[p]roviders of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."* Santos et al. [35] interpreted that this legal provision prohibits three autonomy violation types: *deception, manipulation,* and *distortion/impairment*. Thus, the DSA prohibits dark patterns by explicitly protecting user autonomy [16], articulating autonomy violations [35], and providing examples of potentially prohibited practices in Article 25. Additionally, dark patterns scholarship has identified and taxonomised dark patterns across various contexts. However, there is a gap in situating dark pattern practices within the autonomy violation types outlined in the DSA. To support both online platforms' compliance with the DSA and regulatory enforcement, we argue that it is important to reason about why a given practice would constitute a particular

[1] Inspired by the recent workshop on dark patterns at ACM CHI 2024 [17], we adapt the workshop's statement on the usage of the term "dark patterns". We use this term to connect our efforts to prior scholarship across domains and legal codified concepts, recognizing that other terms, notably "deceptive design" or "manipulative user interface design," are also used but do not yet encapsulate the broad remit of practices or concepts from academic or regulatory perspectives. We acknowledge that the ACM Diversity and Inclusion Council now includes the term "dark patterns" on a list of problematic terms (https://www.acm.org/diversity-inclusion/words-matter).

autonomy violation, to show it can potentially violate DSA Article 25. We argue for methodologies and frameworks to help regulators and online platforms in determining if a given design practice violates user autonomy, and in identifying the type of autonomy violation(s). This work-in-progress builds preliminary steps towards such frameworks, identifying key contributing factors to determine autonomy violation types for a given dark pattern. Specifically, we investigate the following research questions:

(1) **RQ1**: How do currently known dark patterns map to autonomy violation types from Article 25 of the DSA?
(2) **RQ2**: What are the factors which help identify the dark pattern autonomy violations?

We make two contributions. First, we mapped existing dark patterns from the Gray et al. [21] ontology to the three DSA autonomy violation types identified by Santos et al. [35] (Section 3.1). This mapping can enable regulators and platforms to analyse known dark patterns and assess where they violate DSA provisions. Second, we further analysed the corpus of dark patterns to identify factors which contribute to this mapping (Section 3.2). From this analysis, we extracted *8 key factors*. These factors consist of design aspects of the dark patterns which we argue can help establish the reasoning for why a given design practice constitutes a particular type of autonomy violation – deception, manipulation or distortion/impairment (or any combination of these violations) – and hence potentially violates Article 25 of the DSA. Through these contributions, we aim to connect dark patterns knowledge to a legal framework of autonomy violations, both to aid enforcement and DSA compliance.

## 2 Research Methodology

This work leverages authors' expertise in HCI, CS and law. Figure 1 summarizes our qualitative coding methods.

### 2.1 Dark Patterns Dataset and Autonomy Violation Types

*Dark Patterns Dataset.* To map existing dark patterns onto the DSA autonomy violations, we strictly utilize the Gray et al. [21] ontology to center our work, both to align with the broader dark patterns community and to work with a centralized known resource. This ontology consists of 5 high-, 25 meso-, and 34 low-level patterns. The high-level consists of broad design strategies, whereas the low-level specifies the 'means of execution', potentially describing visual and/or temporal elements. The meso-level bridges the high- and the low-levels by describing the 'angle of attack', i.e., the specific approach used to influence users and to undermine their decision making or choice. We exclude the five high-level dark patterns (Obstruction, Sneaking, Interface Interference, Forced Action and Social Engineering) from the analysis, as they do not specify the manner in which a design practice may influence users' choices or decisions. Hence, it was not possible to map them to specific autonomy violations. Then, we map the meso- (N=25) and low-level (N=34) patterns to specific autonomy violations, by analysing the definition of each dark pattern from Gray et al. [21], while using the following interpretations of autonomy from Santos et al. [35].

*Autonomy Violations Prohibited by DSA Article 25.* The DSA in the context of dark patterns prohibits three autonomy violation types: *deception, manipulation* and *distortion/impairment* [35]. **Deception** can be understood as (intentionally or mistakenly) causing someone to have or to sustain a false belief [26]. This includes design practices that create in the user a perception that does not correspond to reality [35]. Mathur et al. [29] argue that dark patterns can cause such deception through affirmative misstatements, misleading statements, or omissions. **Manipulation** is often characterized as a form of influence that is neither coercion nor rational persuasion [33]. Susser et al. [39] explain that *"when we are manipulated, by contrast, we are not constrained. Rather, we are directed, outside our conscious awareness, to act for reasons we can't recognise, and toward ends we may wish to avoid."* Santos et al. [35] interpret that this violation type covers design practices which have a steering effect on users' choices and decisions in a certain direction. **Distortion/impairment** covers influences on autonomy which are neither deceptive nor manipulative, but rather have a forcing or coercive effect [35]. Coercion means influencing someone by constraining their options, so that their only rational course of action is the one intended by the coercer [39, 40]. Hence, this violation type includes design practices that place a set of constraints upon the user, wherein a user acts unwillingly or involuntarily for reasons they can actually recognize or is otherwise prevented from taking an action that they willingly want to take [35].

### 2.2 Coding Procedures

*Autonomy Violation Coding.* We analysed meso- and low-level dark patterns (N=59) from the Gray et al. [21] ontology and assigned to them one or more of the three autonomy violation labels. Initial coding was done independently by two authors (spanning interdisciplinary dark patterns expertise) via AirTable. The two authors coded each dark pattern's autonomy violations as either saw fit, updating both the violation label and secondly providing a short, written explanation for their rationale. We then met to discuss our labels, assessing discrepancies in three rounds.

First, we inspected dark patterns that were assigned a single autonomy violation by both coders (N=22). We were in agreement for 17 patterns, and we discussed the five differing patterns towards consensus, either choosing one best-fit violation type or choosing both violation types. For example, 'Complex Language' dark pattern makes information difficult to understand by using obscure word choices and/or sentence structure [21]. One coder labeled it as deception, and the other as manipulation. At the discussion stage, we concurred on using both labels, as the autonomy violation would depend on whether the use of complex language leads to the creation of false perceptions (deception), or it simply discourages the user from engaging with the information provided (manipulation).

Second, we inspected dark patterns which were assigned a single label by one coder, but multiple labels by the other coder (N=22). For these, we noted that the single label assigned by one coder always appeared as part of the multiple labels assigned by the other coder. We again discussed these patterns towards consensus, either choosing one or multiple violation types which fit best. For example, 'Countdown Timers' dark pattern indicates that a deal or discount will expire by displaying a countdown clock or timer [21].

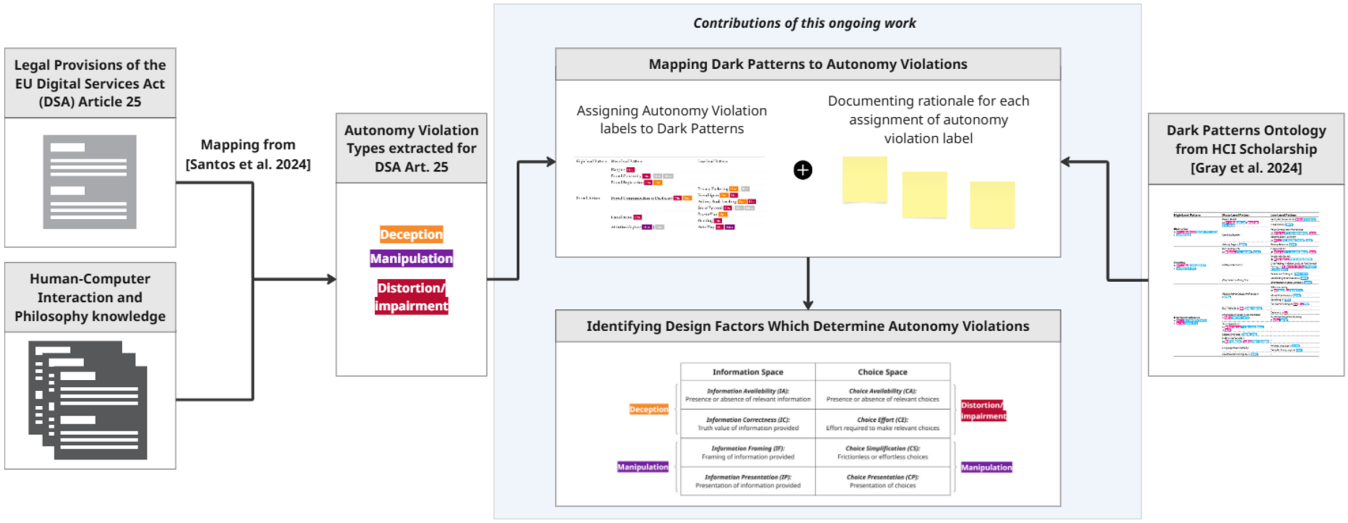


**Figure 1: Methodology used to identify design factors to determine dark pattern autonomy violations**

One coder labeled it as deception, and the other as both deception and manipulation. During discussions, we concurred on using both labels, as the autonomy violation would depend on whether the timer was fake (deception), or it was not fake but it steered the user towards a purchase by creating a sense of urgency (manipulation).

Third and last, we inspected dark patterns which were assigned multiple labels by both coders (N=15). We agreed upon 13 patterns, and we discussed two differing patterns towards consensus. In all three rounds, we documented our shared rationale when deciding the final violation label(s).

*Design Factors Identification.* The aim of this step was to identify the design factors which help determine the dark pattern autonomy violation type(s). At this stage, we excluded the meso-level patterns, as the meso-level definitions describe only an angle of attack, i.e., the approach used to influence users, but do not specify the exact means of execution – making it difficult to infer specific design aspects leading to an autonomy violation (even if the violation type is clear). For this step, the two authors revisited the low-level pattern definitions (N=34), their autonomy violation labels, and the underlying autonomy violation label rationale. We inductively identified and iterated upon the design factors which contributed to our decision to assign particular autonomy violation label(s) to each dark pattern. We refined these factors in discussions with all authors, and we categorised these further into two broad design *spaces*: Information Space and Choice Space. We explain these design factors and spaces in Section 3.2.

# 3 Results

## 3.1 Dark Pattern Autonomy Violations

Our analysis first maps the Gray et al. [21] meso- and low-level dark patterns to one or more of the DSA autonomy violations. Table 1 presents a subset of our results to illustrate the mapping (the full mapping of the 59 dark patterns to autonomy violations is provided in Supplementary Material).

**Single autonomy violation type.** Some dark patterns map to a single type of autonomy violation, either deceiving *or* manipulating *or* distorting/impairing user autonomy. For example, the 'Nagging' dark pattern repeatedly interrupts users [21], leading them to unwillingly make a decision, and we map it to a single autonomy violation type (distortion/impairment).

**Multiple autonomy violation types.** Other dark patterns map to multiple types of autonomy violations. In some cases, the multiple autonomy violations occur *separately*, i.e. one *or* the other. For example, the 'Forced Registration' dark pattern subverts the user's expectation that they can complete an action without registering or creating an account [21]. This expectation can be subverted either by tricking users into thinking that registration is required (deception) or by actually making registration mandatory (distortion/impairment). These violations occur separately, i.e., the pattern *either* deceives *or* distorts/impairs user autonomy.

By contrast, the multiple autonomy violations can also occur *together*. For example, the 'Auto-Play' dark pattern automatically plays new videos for users, forcing them to watch new content (distortion/impairment). However, once a new video has started playing, a user is tempted or steered to continue watching this content, even if they can turn it off (manipulation). Both autonomy violations go hand-in-hand and potentially amplify each other [19].

In some cases, the multiple autonomy violations may also follow a *temporal* progression. For example, in the 'Drip Pricing, Hidden Costs, or Partitioned Pricing' dark pattern [21], if an e-commerce website hides information about full costs of a product or a service, it may constitute deception in the beginning. However, as those costs are revealed later in the user journey, a user may continue with their purchase, not wanting to abandon their progress, which may then constitute manipulation. Therefore, in this case, the initial deception transforms into manipulation based on the temporal progression of the dark pattern.

**Primary and secondary autonomy violations.** For a majority of dark patterns, we could identify the autonomy violations based

on their ontological definitions provided in [21]. These were labeled as *primary* autonomy violations. Moreover, we noted that some dark patterns could implicate additional or supplementary violation types that were not explicitly captured within the definitions, and we labeled these as *secondary* autonomy violations. That is, secondary violations *may potentially* appear in some instances of a given dark pattern, in addition to the primary violation type. 'Forced Continuity' is one such example [21] in which a user's subscription to a service may be automatically renewed, and hence, distortion/impairment is the primary autonomy violation as captured in the pattern definition. However, either deception or manipulation *might be* present depending on the manner in which the information about the auto-renewal was presented to the user. It is important to note that the primary and secondary labeling convention is only with respect to the definition of the dark pattern, and does not relate to any other factors such as importance or severity. Hence, when regulators analyse real-world practices in concrete contexts, the question of primary vs. secondary does not arise, as all dark patterns that are actually present and their autonomy violations are considered primary.

## 3.2 Design Factors to Determine Dark Pattern Autonomy Violations

We identified eight design factors to help determine dark pattern autonomy violation type(s). We further categorised them into two broad design *spaces*: the *Information Space* and the *Choice Space*. The ***Information Space*** consists of all the information made available to the user by an online platform to support user choices and decisions. The ***Choice Space*** consists of the set of choices and options made available to the user by the online platform. This categorisation distinguishes between two sets of design factors: those which influence users by altering information and those which influence users by altering their choice set. We present the eight factors in Figure 2 and explain below how they relate to three autonomy violations.

**Deception.** We identified two design factors, both in the information space, which contribute to deception. These are *Information Availability (IA)* and *Information Correctness (IC)*. Information Availability (IA) is concerned with the *presence or absence of relevant information*, which includes information that pertains to a choice, but also information about the existence of a choice itself. This factor can lead to deception when a design practice omits relevant information entirely or does not provide relevant information at a relevant time or in the relevant context, limiting its discoverability. Information Correctness (IC) is concerned with the *truth value of information provided*. This factor consists of textual information, iconography, graphics, colors, or other forms of information. Any information which is false or misleading can lead to deception.

**Manipulation.** We identified four design factors which can contribute to manipulation. These are: *Information Framing (IF), Information Presentation (IP), Choice Simplification (CS)* and *Choice Presentation (CP)*. In the information space, Information Framing (IF) is concerned with the *framing of information provided*, such as the use of emotionally evocative language, complexity and ambiguity. Information Presentation (IP) is concerned with the *presentation of information provided*, including elements of layout, order, structure, hierarchy or timing of the information provided (without actually omitting any relevant information). Both factors can have a steering effect towards particular choices or options. In the choice space, Choice Simplification (CS) is concerned with *frictionless or effortless choices*. It consists of design practices which remove friction from certain choices, making them too easy or effortless. This absence of friction may steer users towards these choices, but without any added constraints. Lastly, Choice Presentation (CP) is concerned with the *presentation of choices*, including elements of layout, order, structure, hierarchy or timing of the choices presented to the user, which can also steer users towards particular choices or options.

**Distortion/impairment.** We identified two design factors, both in the choice space, which contribute to distortion/impairment. These are: *Choice Availability (CA)* and *Choice Effort (CE)*. Choice Availability (CA) is concerned with the *presence or absence of relevant choices*. It consists of design practices which restrict the user's choice set by omitting relevant choices. It includes practices where certain choices are pre-selected or executed on behalf of the user without any user action. Lastly, it also consists of design practices which mandate or force a user to perform certain actions. Choice Effort (CE) is concerned with the *effort required to make relevant choices*. It consists of design practices which make certain choices unreasonably difficult or effortful. We interpret both these factors as contributing to distortion/impairment, as they introduce constraints that have a forcing or coercive effect on users' decisions.

# 4 Discussion and Future Work

**Implications of our findings.** Our findings showed several dark patterns with more than one autonomy violation types, even though these dark patterns map to the same DSA provision. Triggering multiple violations can have several implications. For example, since there may be a compounded impact on users (purchase decisions, engagement, etc.), companies may be more incentivised to use them. Future works could study if they are even more effective, as users may be more susceptible or vulnerable to dark patterns which operate in multiple ways, even though the extent of this vulnerability depends on the specific practice and its context. In addition, these effects – including dark pattern harms [36] and severity [27] – may be further compounded due to the presence of multiple dark patterns in the same interface [19]. Therefore, we believe that DSA Article 25 enforcement could consider the cumulative impact of multiple dark patterns and multiple autonomy violation types within the same design.

**Future work.** This paper presents an early version of our framework, which we are continuing to refine and develop. Future and longer versions of this paper will include further detail regarding our violation codes and reasoning, as well as deductive coding of each dark pattern according to the design factors implicated in their implementation. We then plan to show how these factors apply to real-world contexts, for example, throughout a user journey, and how they can help in determining autonomy violations. We also aim to validate this framework with the broader interdisciplinary community of dark patterns scholars, and potentially regulators and industry practitioners – ensuring that our inferences are practical, relevant, and effectively address the challenges in enforcement and compliance. Finally, we are interested in applying these factors

**Table 1: Autonomy violation type(s) for a subset of dark patterns**

| High-level Pattern | Meso-level Pattern | Low-level Pattern |
|---|---|---|
| Forced Action | Nagging Dis. | |
| | Forced Continuity Dis. Dec. Man. | |
| | Forced Registration Dis. Dec. | |
| | Forced Communication or Disclosure Dis. Dec. | Privacy Zuckering Dec. Dis. |
| | | Friend Spam Dec. Dis. |
| | | Address Book Leeching Dec. Dis. |
| | | Social Pyramid Dis. Dec. Man. |
| | Gamification Dis. | Pay-to-Play Dec. |
| | | Grinding Dis. |
| | Attention Capture Man. Dec. | Auto-Play Dis. Man. |

Dec. = Deception; Man. = Manipulation; Dis. = Distortion/impairment; Greyscale label represents secondary autonomy violation

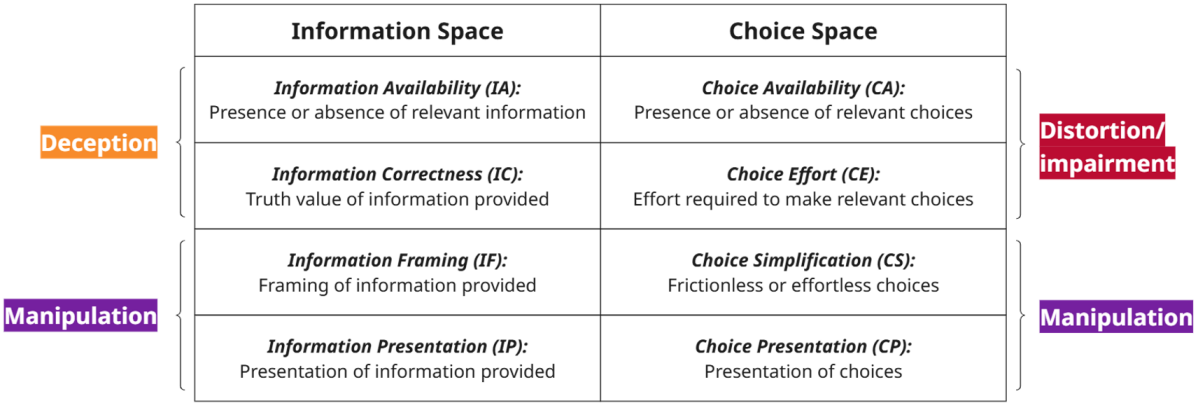


**Figure 2: Design factors which help determine the dark pattern autonomy violation type(s)**

to the legal cases currently facing the EU Commission, to show how our framework assists in determining autonomy violations for the given dark patterns.

We believe that our framework could help EU data protection, consumer and DSA regulators with determining autonomy violations and their underpinning design factors in dark patterns. These inferences can be complemented by user studies that show how dark patterns influence user behavior, and thus demonstrate these autonomy violations in action [3, 38]. As such, this framework would benefit from future cross-cultural analyses, as autonomy violations might be perceived differently by regulators and users across various European countries implementing the DSA. Lastly, as the DSA is enforced, we expect that the usage and prevalence of such design practices will change over time. Hence, future work may also focus on longitudinal studies measuring the impact of regulatory pressure and enforcement on the evolution of dark patterns.

## 5 Conclusion

This work represents a transdisciplinary contribution from the HCI community for policymaking. Alongside the European Commission's ongoing formal proceedings pertaining to DSA Article 25 violations [11, 12], we anticipate further regulatory actions in the EU against dark patterns in online platforms. As the three DSA autonomy violations are broadly formulated, they are open to interpretation, even from different disciplines (philosophy, HCI, law). Hence, our identified factors concretely articulate which design aspects lead to a particular dark pattern autonomy violation type. Our findings suggest that *deception* occurs due to factors related to the information provided to users (*Information Space*), while *distortion/impairment* occurs due to factors related to users' choice set (*Choice Space*). Whereas, *manipulation*, as a steering effect, can occur in both information and choice spaces. We argue that the *8 key factors* identified in this paper offer valuable insight from HCI, complementing the DSA legal framework to enable its practical implementation.

## Acknowledgments

This work has been supported by the ANR 22-PECY-0002 IPoP (Interdisciplinary Project on Privacy) project of the Cybersecurity PEPR, Inria DATA4US Exploratory Action project, and the Inria International Chair funding.

## References


[1] Sanju Ahuja and Jyoti Kumar. 2022. Conceptualizations of user autonomy within the normative evaluation of dark patterns. *Ethics and Information Technology* 24, Article 52 (2022). doi:10.1007/s10676-022-09672-9

[2] Sanju Ahuja and Jyoti Kumar. 2024. Layered Analysis of Persuasive Designs: A Framework for Identification and Autonomy Evaluation of Dark Patterns. In *Proceedings of the Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024) Workshop at CHI conference on Human Factors in Computing Systems* (Honolulu, HI, USA). Article 1, 14 pages. https://ceur-ws.org/Vol-3720/paper1.pdf

[3] Nataliia Bielova, Laura Litvine, Anysia Nguyen, Mariam Chammat, Vincent Toubiana, and Estelle Hary. 2024. The effect of design patterns on (present and future) cookie consent decisions. In *Proceedings of the 33rd USENIX Conference on Security Symposium* (Philadelphia, PA, USA) *(SEC '24)*. USENIX Association, USA, Article 158, 18 pages.

[4] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 237–254. doi:10.1515/popets-2016-0038

[5] Harry Brignull. 2018. Deceptive Patterns: User Interfaces Designed to Trick People. http://darkpatterns.org/

[6] Harry Brignull. 2023. Deceptive Patterns. https://www.deceptive.design

[7] Akash Chaudhary, Jaivrat Saroha, Kyzyl Monteiro, Angus G. Forbes, and Aman Parnami. 2022. "Are You Still Watching?": Exploring Unintended User Behaviors and Dark Patterns on Video Streaming Platforms. In *Proceedings of the 2022 ACM Designing Interactive Systems Conference* (Virtual Event, Australia) *(DIS '22)*. Association for Computing Machinery, New York, NY, USA, 776–791. doi:10.1145/3532106.3533562

[8] CMA 2022. *Evidence review of Online Choice Architecture and consumer and competition harm.* Technical Report. https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers/evidence-review-of-online-choice-architecture-and-consumer-and-competition-harm

[9] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3313831.3376600

[10] DSA 2022. 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) (Text with EEA relevance). http://data.europa.eu/eli/reg/2022/2065/oj

[11] European Commission 2024. Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373

[12] European Commission 2024. Commission sends preliminary findings to X for breach of the Digital Services Act. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761

[13] European Data Protection Board. 2023. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them.* Technical Report Version 2.0. https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[14] Dan Fitton and Janet C. Read. 2019. Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children* (Boise, ID, USA) *(IDC '19)*. Association for Computing Machinery, New York, NY, USA, 407–418. doi:10.1145/3311927.3323136

[15] FTC 2022. *Bringing Dark Patterns to Light Staff Report.* Technical Report. Federal Trade Commission. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

[16] Maximilian Gartner. 2022. Regulatory Acknowledgment of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act. *European Data Protection Law Review* 8, 4 (2022). doi:10.21552/edpl/2022/4/6

[17] Colin M. Gray, Johanna T. Gunawan, René Schäfer, Nataliia Bielova, Lorena Sanchez Chamorro, Katie Seaborn, Thomas Mildner, and Hauke Sandhaus. 2024. Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 482, 6 pages. doi:10.1145/3613905.3636310

[18] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3173574.3174108

[19] Colin M. Gray, Thomas Mildner, and Ritika Gairola. 2025. Getting Trapped in Amazon's "Iliad Flow": A Foundation for the Temporal Analysis of Dark Patterns. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 225, 10 pages. doi:10.1145/3706598.3713828

[20] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 2021. Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 172, 18 pages. doi:10.1145/3411764.3445779

[21] Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, and Thomas Mildner. 2024. An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 289, 22 pages. doi:10.1145/3613904.3642436

[22] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 377 (Oct. 2021), 29 pages. doi:10.1145/3479521

[23] Johanna Gunawan, Cristiana Santos, and Irene Kamara. 2022. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. In *Proceedings of the 2022 Symposium on Computer Science and Law* (Washington DC, USA) *(CSLAW '22)*. Association for Computing Machinery, New York, NY, USA, 181–194. doi:10.1145/3511265.3550448

[24] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a Light on Dark Patterns. *Journal of Legal Analysis* 13, 1 (March 2021), 43–109. doi:10.1093/jla/laaa006

[25] Francisco Lupiáñez-Villanueva, Alba Boluda, Francesco Bogliacino, Giovanni Liva, Lucie Lechardoy, and Teresa Rodríguez de las Heras Ballell. 2022. *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report.* Publications Office of the European Union, Brussels, Belgium. doi:10.2838/859030

[26] James Edwin Mahon. 2016. The Definition of Lying and Deception. In *The Stanford Encyclopedia of Philosophy* (Winter 2016 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University.

[27] Gianclaudio Malgieri and Cristiana Santos. 2025. Assessing the (severity of) impacts on fundamental rights. *Computer Law & Security Review* 56 (2025), 106113. doi:10.1016/j.clsr.2025.106113

[28] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 81 (Nov. 2019), 32 pages. doi:10.1145/3359183

[29] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 360, 18 pages. doi:10.1145/3411764.3445610

[30] Thomas Mildner, Merle Freye, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. 2023. Defending Against the Dark Arts: Recognising Dark Patterns in Social Media. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 2362–2374. doi:10.1145/3563657.3595964

[31] Thomas Mildner, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. 2023. About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 192, 15 pages. doi:10.1145/3544548.3580695

[32] Carol Moser, Sarita Y. Schoenebeck, and Paul Resnick. 2019. Impulse Buying: Design Practices and Consumer Needs. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. doi:10.1145/3290605.3300472

[33] Robert Noggle. 2022. The Ethics of Manipulation. In *The Stanford Encyclopedia of Philosophy* (Summer 2022 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University.

[34] OECD. 2022. *Dark commercial patterns.* Technical Report. doi:10.1787/44f5e846-en

[35] Cristiana Santos, Nataliia Bielova, Sanju Ahuja, Christine Utz, Colin Gray, and Gilles Mertens. 2024. Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA? Available at SSRN: https://ssrn.com/abstract=4899559.

[36] Cristiana Santos, Viktorija Morozovaite, and Silvia De Conca. 2025. No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Information & Communications Technology Law* (2025), 1–47. doi:10.1080/13600834.2025.2461958

[37] Brennan Schaffner, Neha A. Lingareddy, and Marshini Chetty. 2022. Understanding Account Deletion and Relevant Dark Patterns on Social Media. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 417 (Nov. 2022), 43 pages. doi:10.1145/3555142

[38] Brennan Schaffner, Yaretzi Ulloa, Riya Sahni, Jiatong Li, Ava Kim Cohen, Natasha Messier, Lan Gao, and Marshini Chetty. 2025. An Experimental Study Of Netflix Use and the Effects of Autoplay on Watching Behaviors. In *2025 ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW 2025)*. Accepted for publication.

[39] Daniel Susser, Beate Roessler, and Helen Nissenbaum. 2019. Technology, autonomy, and manipulation. *Internet Policy Review* 8 (2019). Issue 2. doi:10.14763/2019.2.1410

[40] Allen W. Wood. 2014. Coercion, Manipulation, Exploitation. In *Manipulation: Theory and Practice*, Christian Coons and Michael Weber (Eds.). Oxford Academic, New York, 274–302. doi:10.1093/acprof:oso/9780199338207.001.0001

[41] José P Zagal, Staffan Björk, and Chris Lewis. 2013. Dark patterns in the design of games. In *Foundations of Digital Games 2013.* https://www.diva-portal.org/smash/get/diva2:1043332/FULLTEXT01.pdf