SciencesPo

CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

How should the European Union regulate dark patterns?

Thomas Akhurst, Laura Zurdo

Riccardo Rapparini & Christoph Mautner Markhof

Comparative Approach to Big Tech Regulation (Spring 2023)

Professor Florence G'sell

April 2023

Abstract

In November 2022, the European Union (EU)'s Digital Services Act (DSA) entered into force. It imposes new duties on online intermediaries aiming to protect users' fundamental rights online. Among a range of rules, Article 25 establishes a prohibition against dark patterns. This policy brief analyses the DSA's approach to dark patterns through the following research question:

"How should the Digital Services Act's prohibition on dark patterns be implemented?"

After introducing the policy context in Section 1 and offering a descriptive analysis of the DSA and its antecedents with regard to dark patterns in Section 2, Section 3 will analyse four issues of relevance to Article 25's implementation. These findings aim to steer the European Commission's (EC, or the Commission) implementation of Article 25 DSA, highlighting four areas that the Commission must address, whether through guidelines on Article 25 and/or through delegated acts. The discussion will be structured according to the logic of concentric circles, expanding from a narrow to a wide perspective. The first issue discussed—"legal definitions"—explores uncertainties in the terms contained within the Article. The second issue—"legal scope"—zooms out of Article 25 to assess how it might interact with pre-existing regulation of dark patterns, specifically the General Data Protection Regulation (GDPR) and Unfair Commercial Practices Directive (UCPD). Our third issue looks beyond legal meanings to practical implications of enforcement; namely, in what ways Article 25 impacts *who* enforces dark pattern prohibitions and *how* they do so. The fourth issue takes a holistic view of the DSA, exploring provisions outside Article 25 that could be used to address dark patterns. Finally, Section 5 presents a series of recommendations.

1. Clarify terms: (i) manipulative interface personalisation would be better addressed by strengthening GDPR data protection, (ii) a *potential* deceitful effect should be enough to meet Article 25 (iii) the standard used to assess if a practice is likely to deceive should be lower than the average consumer, to account for digital asymmetries.
2. Clarify scope: Define the interplay of the scopes of the DSA, UCPD and GDPR.
3. Coordinate enforcement, especially between Digital Service Coordinators and consumer authorities.
4. Harness the full "DSA toolbox", as there are other provisions within the DSA that can be used to tackle dark patterns, beyond the Article 25 prohibition.

Table of contents

1.1. Context — dark patterns as a policy issue

Dark patterns are a serious and pervasive threat to core liberal democratic principles. Coined by designer Harry Brignull in 2010 (Sinders, 2021), the term refers to online interface designs that aim to manipulate users into acting against their own interests, usually for the benefit of the relevant website or app provider (Luguri & Strahilevitz, 2021). While the term is loosely defined, regulatory action against dark patterns originates in the intuition that individuals should be free to assess and define their own interests in a democratic society. Democracy is premised on the decentralisation of power and the protection of individual rights, but dark patterns transform online interfaces into biased architectures that privilege and amplify the interests of online platforms. The Digital Services Act (DSA) reflects these sentiments aiming to guarantee an "online environment (that protects) [...] fundamental rights […] in particular the freedom of expression, [...] the right to non-discrimination and […] a high level of consumer protection" (recital 3). Action against dark patterns is therefore an important constitutive part of the broader effort to build a digital society fit for liberal democracy.

Dark patterns have been prohibited through various EU legislative instruments, including the Unfair Commercial Practices Directive (UCPD) and General Data Protection Regulation (GDPR). The main rationale for dark patterns regulation is represented by the right to respect for family life (Article 7 EU Charter) which underpins the protection of individual autonomy (Gumbis et al., 2008) – or the capacity to align one's actions with one's true preferences (Yeung, 2017). However, their presence has been far from averted. The European Commission and the European Consumer Protection Network recently performed a screening of retail websites, focusing on three types of dark patterns, and found that 40% of the screened retailers used them (European Commission, 2023). In a separate study, the EC found that 97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern (Lupiáñez-Villanueva et al., 2022).

Some critics argue that dark patterns persist because dark pattern regulation has typically focused on 'static' features (i.e. easily observable interface features that are not personalised to users), while online manipulation is increasingly 'dynamic' (i.e. result from the use of data to personalise interfaces in a way that manipulates user behaviour) (Yeung, 2017). In a similar vein, some claim that the EU needs additional regulation that is better fitted for the digital age (BEUC, 2022). Others have countered that the reason why dark patterns prevail in the EU is mainly due to deficiencies in the framework's enforcement, rather than because of lack of regulation (Ecommerce

Europe, 2022). One thing is for certain, dark patterns are a continuing, prominent, and increasingly problematic characteristic of online life.

It is in this context that a new prohibition against dark patterns has entered into force through Article 25 of the DSA. The next step and most urgent task in the context of European digital regulation of dark patterns, is determining how the DSA can best be implemented. This policy brief analyses this issue, highlighting four areas that the European Commission must address to best harness the DSA's potential regarding the restriction of dark patterns. The Commission is best positioned to receive these recommendations, given its ability to produce guidelines on the Article 25 prohibition (Article 25(3) DSA).

2.2. Legal framework — how has the EU regulated dark patterns?

The DSA is not the first EU legislative act to prohibit dark patterns. This section lays out the key provisions in EU law used to tackle them, reviewing the legal instruments that preceded the DSA before analysing its addition, Article 25 DSA.

2.1. Before the Digital Services Act

Prior to the DSA, EU law addressed dark patterns chiefly through data and consumer protection law. In particular, the General Data Protection Regulation (GDPR) and the Unfair Commercial Practices Directive (UCPD) have played prominent roles, despite that neither of them expressly mentions dark patterns.

2.1.1. General Data Protection Regulation

The GDPR[1] regulates the protection of personal data, defined as "any information relating to an identified or identifiable natural person". It applies to all processing of personal data carried out by data controllers or processors that offer goods or services to individuals in the EU or monitor their behaviour. In this sense, the GDPR applies regardless of the controller's place of establishment, within or outside the EU. The Regulation also provides data subjects with a set of rights, particularly to information and control about how their data is processed.

Data processing activities must be fair (Article 5(1)(a) GDPR) and based on one of the six grounds for legitimate processing provided in the Regulation (Article 6(1)). One ground for legitimate processing is where it occurs with the relevant data subject's consent. Under Article 4(11) GDPR, to obtain legitimate consent from a data subject,

the consent must be free, specific, informed, and unambiguous. However, data controllers have often developed confusing user interface designs that inhibit a data subject's ability to provide consent freely and legitimately (Sinders, 2021), countering both Article 4(1) GDPR and the general fairness principle contained in Article 5 GDPR (European Commission 2021).

To prevent these practices, the GDPR *bans online interfaces aimed at misleading the user into agreeing to more processing than what is in their best interest* (Luguri & Strahilevitz, 2021). For example, the European Court of Justice (ECJ) has held that a pre-ticked box cannot constitute valid consent (Case C-673/17 *Planet49 GmbH*). Similarly, consent is invalid if the ability to object to data collection and storage is "unduly affected" by the need to "complete an additional form setting out that refusal". In other terms, both the "yes" and "no" options on a cookie form must be equally accessible (European Court of Justice, Case C-61/19 *Orange Romania*, para. 53).

Further, the European Data Protection Board (EDPB, 2022) has adopted Guidelines on dark patterns in social media platform interfaces, laying out best practices for designers. The Guidelines outline six categories of patterns that infringe the GDPR: overloading (overwhelming users with voluminous information or possibilities), skipping (prompting users to overlook or forget relevant privacy considerations), stirring (appealing to emotions or using visual nudges to shape choices), hindering (making data management difficult or impossible), fickle (unclear interfaces designed to confuse the user), and left in the dark (hides relevant information or data protection tools).

2.1.2. Unfair Commercial Practices Directive

In EU law, the UCPD[2] provides the general framework for regulating commercial practices in *business-to-consumer* (B2C) relationships, prohibiting practices deemed unfair. The UCPD applies to a wide range of practices by any trader involved in the promotion, sale, or supply of a product or service to consumers (Article 2(d) UCPD). On one hand, a trader is any natural or legal person who acts in their own name for purposes related to their business, or anyone acting on a trader's behalf (Article 2(b) UCPD). Charitable organisations and public authorities can be traders when they engage in commercial activities towards consumers, like an NGO selling products that meet certain ethical standards (European Commission, 2021, p. 28). On the other side, a consumer is "a natural person, who [acts] outside the scope of an economic activity (trade, business, craft, liberal profession)" (Article 2(a) UCPD).

A commercial practice may range from an action to an omission, and even to communications such as marketing. It can take place before, during, or after a commercial transaction. Accordingly, the UCPD does not require a purchase or a contractual relationship, so long as the practice is directly related to the promotion of a

product or service to consumers (European Commission, 2021). To be deemed unfair, the practice must be *likely to cause a consumer to make a transactional decision that they would not have otherwise made*. Transactional decisions include, beyond purchases, any other choices directly related to it, like the choice to enter a shop (European Court of Justice, Case C-281/12 *Trento Sviluppo srl*, para. 35). Unfair practices may arise if they breach the trader's professional diligence (Article 5 UCPD), if they are misleading (Article 6 UCPD) or aggressive (Articles 8 and 9). Misleading practices hide or present information in a way that leads consumers to make a decision they would not have otherwise made. Conversely, aggressive practices involve harassment or coercion. In all cases, the trader's intention to deceive is not required.

To apply the UCPD, enforcers check if the practice is blacklisted in the UCPD's Annex I. If not, they evaluate it case-by-case. As mentioned, the key issue is the practice's likelihood of leading consumers to making an unwanted transactional decision. Generally, commercial practices are evaluated from the perspective of the average consumer, who is "reasonably well informed, observant and circumspect" (European Court of Justice, Case C-210/96 *Gut Springenheide and Tusky*, para. 31). However, a practice that targets a vulnerable consumer is assessed from their specific point of view. Vulnerability may arise from permanent characteristics like age, mental, or physical infirmity, or be context-dependent (European Commission, 2021, p. 35).). For instance, the unfairness of a practice that targets children is assessed considering that children process information differently (ACM, 2022, p. 15).

The UCPD is technologically neutral, applying offline and online. The Commission's 2021 Guidelines on the UCPD assess its application to digital environments. Importantly, practices within *B2C relationships where customers make no monetary payment but which generate another benefit for the trader, like the monetisation of user data, fall within the umbrella of commercial practices* (ACM, 2022, p. 14). Customers' transactional decisions in the online sphere include the choice to access a website, to continue using a service (e.g., feed scrolling), to click a link, or to view advertisements (European Commission, 2021, p. 100).

The Guidelines dedicate a section to dark patterns, noting that dark patterns in a B2C relationship can be challenged under the UCPD. Annex 1 directly blacklists certain dark patterns, including bait and switch, fake limited stock claims, fake timers, and nagging. For other patterns, the UCPD's general logic would apply: a dark pattern is a *misleading* practice if it hides relevant information or provides it in a way that leads the consumer to make a decision they would not have taken, absent that pattern. Alternatively, it is *aggressive* if it significantly impairs consumers' freedom of choice, through coercion or undue influence, causing them to take an unwanted decision. For example, a trader's online interface that makes terminating a contract more difficult than entering it (e.g., hidden behind several screens or confusing options), would be engaging in a prohibited dark pattern (European Commission, 2021, p. 102). Similarly, a dark pattern that hides

additional unavoidable booking fees constitutes a misleading commercial practice, prohibited under the UCPD (Dutch Trade and Industry Appeals Tribunal, Case 17/1179 *ACM/Corendon*).

2.1.3. Other

Beyond the GDPR and UCPD, other instruments directly or indirectly refer to dark patterns. Firstly, the *Unfair Contract Terms Directive*[3] protects consumers from unfair and not individually negotiated contractual terms. A contract may be void if its terms are presented unclearly, using dark patterns to imbue confusion through visual interference (BEUC, 2022, p. 11). Similarly, the *Consumer Rights Directive* requires that consumers are able to understand the consequences of concluding a contract (BEUC, 2022, p. 9). Additionally, under the *ePrivacy Directive*[4], consumers must consent to any cookies in their terminal equipment, and misleading interfaces may contravene the attainment of legitimate consent (European Commission, 2022, p. 75).

Recent and upcoming legislation may also be relevant. For instance, Article 7 of the *Digital Markets Act (DMA)* bans gatekeepers from using dark patterns to circumvent their DMA obligations. Furthermore, Article 5(1)(a) of the proposed *Artificial Intelligence (AI) Act* similarly prohibits the use of AI systems to *deploy "subliminal techniques* (...) *to materially distort* [users'] *behaviour"* likely causing them harm.

2.2. The DSA prohibition: Article 25

On the 1st of November 2022, the EU's Digital Services Act entered into force. The DSA regulates the provision of online intermediary services in the EU, impacting the regulation of dark patterns. Most prominently, Article 25 DSA prohibits the use by online platforms of deceitful or manipulating interfaces, a term that—as recital 67 illustrates—encompasses dark patterns. This prohibition was absent in the Commission's initial proposal. However, it was added by the Council and Parliament during the trilogue negotiations (BEUC, 2022, p. 12).

Under the rubric "online interface design and organisation", Article 25(1) DSA prohibits online platforms from *"design[ing], organi[sing], or operat[ing] their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of the service to make free and informed decisions".* Article 25 provides three specific examples:

- "Giving more prominence to certain choices when asking the recipient […] for a decision",

- "Repeatedly requesting that they recipient […] make a choice where that choice has already been made", and
- "Making the procedure for terminating a service more difficult than subscribing to it".

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

- "Giving more prominence to certain choices",
- "Repeatedly requesting a recipient of the service to make a choice where such a choice has already been made",
- "Making the procedure of cancelling a service significantly more cumbersome than signing up to it",
- "Making certain choices more difficult or time-consuming than others",
- "Making it unreasonably difficult to discontinue purchases or to sign out from a given online platform", and
- "Default settings that are very difficult to change".

2.2.1. Subjective scope—who does the prohibition apply to?

The prohibition on dark patterns extends only to *online platforms*; defined as intermediary service providers who host user-generated information and disseminate it to the public at the user's request (Article 3(i) DSA, recital 13). Public dissemination occurs when such information is made available to a potentially unlimited number of people, regardless of how many actually access it (recital 14). The prohibition applies regardless of the platform's place of establishment, so long as it provides services to users in the EU (Article 2(1)). Nevertheless, to avoid imposing disproportionate obligations, the prohibition does not apply to micro or small enterprises (Article 19), nor to intermediaries who only publicly disseminate user content as an ancillary feature (Article 3(i)). At the other end are *"recipients of the service"*, who may be all sorts of users, including both consumers and business users (Article 3(b), recital 2).

2.2.2. Objective scope—what conduct does it prohibit?

The DSA prohibits design choices or user interface experiences on online platforms that manipulate or deceive users in a way that *impairs their autonomy*. In establishing autonomy as its benchmark, Article 25 targets practices that *nudge a recipient into a choice contrary to their preferences*; or *impair* the exercise of autonomy such that the user is unable to define their own preferences. Intermediaries may impair user choices through "the structure, design or functionalities of an online interface" (recital 67), and hence Article 25 forbids the manipulative "design, organisation and operation" of such interfaces.

Another element of the prohibited conduct is that its effect of deceiving or manipulating recipients must be *"material".* The DSA itself does not clarify if the effect must be actual or if a *potential* effect may suffice. Nor does it clarify what materiality is. A related question is what the recipient standard should be when evaluating whether a practice is deceptive: how savvy must the recipient be? Should the UCPD's "average consumer" standard be used? Finally, Article 25(2) clarifies that the DSA prohibition *shall not apply to practices covered by the GDPR and the UCPD*. This begs the question of what scope is left for the DSA prohibition. These crucial questions will be discussed in Section 3.

2.2.3. Enforcement – how will it be enforced?

As laid out in Article 38 DSA, each member state appoints their own Digital Services Coordinator (DSC) who is responsible for the enforcement of the Act's prescriptions. The DSC acts independently from other authorities or private parties (Article 39), and exerts its supervision with respect to platforms established in the respective member state (Article 40).

National DSCs are conferred with three different types of power, namely investigation, enforcement and further powers such as applying for injunctions (Cauffman & Goanta, 2021). Their enforcement power translates to the authority to make compliance agreements, impose fines and other interim measures (*ibid.*). Furthermore, the DSA provides for the creation of a European Board for Digital Services which advises the national DSCs (Article 47). Competences for conduct investigation and the imposition of sanctions are also conferred to the European Commission in the context of very large online platforms (VLOPs) (Article 51). Hence, both the Commission and Digital Service Coordinators can conduct on-site inspections, request data from platforms, as well as conduct interviews (*ibid.)*.

The enforcement of the DSA is based on the imposition of fines to deter companies from non compliance. The penalties are to be determined by national law, with a maximum ceiling of 6% of the total yearly revenues (Article 42(3)). In specific cases, other types of fines can be imposed albeit also being subject to imposable limits

determined by the DSA. Furthermore, fines can be imposed by the European Commission mirroring this system (Article 59).

Aside from penalties for non-compliance, there are also some mechanisms aimed at increasing the compliance of VLOPs and VLOSEs. Among these, there is the obligation to appoint a compliance officer (Article 41), as well as to conduct independent yearly audits (Article 37). Furthermore, the Commission may request VLOPs to delineate and share an action plan aimed at ensuring respect for DSA rules (Article 75). Voluntary codes of conduct at the Union level are also a part of the DSA's enforcement, and their creation and definition are supported by both the Commission and the European Board of Digital Services as defined under Article 45. In this context, codes of conduct aim to guarantee consistent application of the framework fostering regulatory harmonisation.

3.3. Key issues in Article 25 DSA

This section outlines four key issues that the European Commission should address to maximise the potential of the DSA, particularly of Article 25, for tackling dark patterns. First, this section considers uncertainties in some legal terms. Second, it highlights unresolved questions of Article 25's legal scope, namely uncertainties around the DSA's interaction with the UCPD and GDPR. Third, we address enforcement challenges. Finally, because Article 25 is only one of many provisions in the DSA, this brief contemplates potentially overlooked opportunities to use the DSA in whole (as a "toolbox") to tackle dark patterns. The Commission is in an ideal position to address these areas, given its ability to publish guidelines on the Article 25 prohibition (Article 25(3) DSA).

This policy brief understands implementation to be optimal if it meets three related objectives:

i. Ensuring a *consistent EU legal framework* on dark patterns and *legal certainty* about how the regulatory instruments interact (*Issues 1* and *2*).

ii. Procuring *effective enforcement* of this framework, including Article 25 (*Issue 3*).

iii. Maximising the DSA's *utility* regarding dark patterns, highlighting other articles that can be used to tackle them (*Issue 4*).

These objectives are to be seen as necessary conditions to ensure the sustainability and effectiveness of the EU's legal framework. As the DSA is part of the EU's legal acquis, its dispositions and related effects must fit with the EU's broader legal framework. Only this way can the EU's objectives, including the fostering of the Single Market and the protection of EU citizens' rights (Article 3 Treaty on European Union),

be achieved. In addition, given the DSA's role in achieving the Commission's vision for Europe's digital future, its implementation must be aligned with the inter-institutional solemn declaration on digital rights and principles for the digital decade. In this context, ensuring legal consistency and effective enforcement is key in achieving the principles of 'people at the centre', 'freedom of choice' and 'safety and security' (European Commission, 2022).

3.1. Legal definitions

There are three main definitional uncertainties that each create their own risks or relevant issues. First, the terms "interface design, operation and organisation"—Article 25's definition of prohibited online interfaces is vague and could be interpreted to encompass aspects of online architecture that have not traditionally been treated as dark patterns. Second, it is unclear whether the DSA prohibition includes potential, as well as actual, deceit. Third, the recipient standard is unsettled; according to which standard will the DSA assess interfaces as manipulative and/or deceptive?

3.1.1. Prohibited conduct: does it cover manipulation through interface personalisation?

As Section 1 introduced, most approaches to dark patterns have been definitionally confined to relatively observable interface features. This can include the equal presentation of 'yes' and 'no' options on cookie consent forms, or countdown timers that create a false impression of urgency to encourage purchases. However, critics argue that this approach fails to account for emergent forms of user manipulation that occur through interface personalisation. It has inspired calls for an expanded understanding of manipulative practices, with some positing that the issue should no longer be framed as "dark patterns" but through broader conceptualisations like manipulative online choice architectures (Ecommerce Europe, 2022), to account for more dynamic practices such as behavioural algorithms.

Manipulative personalised interfaces leverage behavioural science to target individualised biases, prompting users to act against their own interests for the benefit of the relevant company. The novelty of manipulation through interface and UX personalisation is that it is not observable to the naked eye. As the European Consumer Organisation (BEUC) explains, "the use of technology and behavioural experimentation on choice architecture… coupled with the collection of vast amounts of data revealing consumers' most personal characteristics, enables businesses to identify which decision leads to which change in user behaviour" (2022, p. 4). The EC's own *Behavioural study on unfair commercial practices in the digital environment* found that "the combination of classic dark patterns with personalisation techniques… (is) a new

frontier… leading to commercial practices that are more difficult to recognise and regulate" (2022, p. 60).

Existing approaches to dark patterns—which tend to focus on the static or observable aspects of interface design—are ill-equipped to address manipulation through interface personalisation. Under the UCPD, this limitation is embodied by the fact that it assumes an average consumer standard divergent to the realities of "digital asymmetry" (BEUC, 2022, p. 9). This standard does not acknowledge the inherently manipulative effects of "algorithms (used) by businesses to target their choice architecture to a consumer (in a way that shapes) individual decision making" (BEUC, p. 4). What's more, in placing its burden of proof on the complainant, the UCPD makes it difficult to prosecute personalisation practices that are known only by the companies or hidden behind algorithmic opacity. The EC itself has argued that legislative changes are needed "despite the presence of a strong EU legal framework (...) to better respond to dark patterns and manipulative personalisation" (Lupiáñez-Villanueva et al., 2022, p. 7).

With this in mind, the wording of Article 25 and its associated recital is potentially interpretable to encompass emergent dynamic practices. Although the prohibited examples described explicitly in Article 25 align with the traditional static definition of dark patterns, it is notable that the article does not adopt the term "dark patterns". Rather, it opts for the broader terminology of "online interface and design". As a result, it is unclear what Article 25 intends when it says that "...online platforms shall not *design, organise or operate* their online interfaces in a way that deceives or manipulates…" (Article 25(1) DSA). To a similar effect, what does recital 67 intend when it refers to the prohibited "*structure, design or functionalities* of an online interface"? These terms ("design", "organise", "operate", "structure", and "functionalities") are potentially broadly interpretable beyond static interface features to dynamic dark patterns based on personalisation.

Given that the Article 25 prohibition was implemented to address "gaps" in dark pattern regulation, it is plausible that the DSA intends to address manipulative interface personalisation as a dark pattern. As noted above, the DSA prohibition refers not just to the design and functionalities of an online interface, but also to operations and structures that deceive and/or manipulate. The DSA's emphasis on manipulation and autonomy is also instructive, as these are paramount consequences of interface personalisation. Nonetheless, these questions remain unclarified.

3.1.2. Deceitful effect: actual or potential?

As mentioned, Article 25 does not clarify whether the effect of deceiving the user needs to be actual or potential. In the pre-DSA regulation of dark patterns, a potential effect has been sufficient. As noted in Section 2.1, the UCPD does not require any demonstration that a consumer was effectively deceived; only proof that the pattern

was likely to have that effect. Given the UCPD and the DSA share a common objective to eliminate dark patterns, they could be interpreted in a complementary way. In other words, the DSA could share the UCPD's approach that makes actual and potential deception both subject to the prohibition. A complementary interpretation would also help determine what Article 25 intends in stating that the system design or user interface must *materially* distort the user's choice, because a materiality requirement also exists in the UCPD. In this case, EC guidelines show that—under the UCPD— the practice must be *likely to cause* the recipient to make a decision that they would not have otherwise taken (European Commission, 2021, p. 31).

3.1.3. Recipient standard: average consumer or vulnerable user?

The text of Article 25 does not specify what recipient standard will be used to determine whether a pattern is likely to deceive users. Here, a complementary approach with the UCPD could also be possible. This would imply using the *average consumer* as a general standard, except when a practice is directed as a particular vulnerable group (see Section 2.1).

Alternatively, the Commission could take a different approach to the UCPD in clarifying the DSA's definition of a recipient standard. Here, the criticisms of EU consumer law discussed above are relevant. Once again, the problem stems from using an "average consumer" benchmark that does not account for the digital asymmetry between parties in dark patterns (Helberger et al., 2021; BEUC, 2022). As a result, BEUC has proposed changing the standard to account for the weaker side's vulnerability. BEUC notes that "the trader has access to the consumer's detailed personal profile, including decision-making biases. [Simultaneously], the trader controls and shapes the entire environment in which the consumer operates". Under these conditions, "all digital consumers are rendered vulnerable" (BEUC, 2022, p. 10) and universally susceptible "to the exploitation of power imbalances" (Helberger et al., 2021, p. 1). In such a case, "vulnerability as an exception becomes less useful to assess the behavioural distortion that an interface can cause" (BEUC, 2022, p. 10). While BEUC's critiques were made in the context of the UCPD, they can inform the Commission's analysis of the appropriate recipient standard within Article 25 of the DSA.

Lowering the DSA's recipient standard below the current UCPD "average consumer" benchmark would ease the burden of proof for demonstrating that a platform's design choice constitutes an illegal dark pattern. There is an established basis for this in the DSA, as the Act expressly articulates a core aim to tackle information asymmetries between users and platforms, and increase the agency of citizens and businesses when they interact with platforms' environments (DSA Impact Assessment, paras. 90 and 217). Recital 67 itself acknowledges that dark patterns often prey on behavioural biases; this might render ideas of a rational and observant consumer as incompatible with the realities of dark patterns. Even in consumer law, the Commission seems to be

moving towards an acknowledgement of these asymmetries.[5] However, there is some disagreement among observers. Sceptics have cautioned against unlimited relaxation of the legal standards, citing the difficulty involved in distinguishing legitimate persuasion from illegitimate manipulation. They warn that "if everything is a dark pattern then nothing is a dark pattern" (Goanta & Santos, 2023, n.d.).

3.2. Legal scope

Effective regulation of dark patterns also requires legal certainty. As such, the Commission must urgently clarify the scope of the key components of the legal framework. Currently, the interplay between the DSA and pre-existing legal instruments is unclear and can lead to confusion about how to take action against a given dark pattern. The ambiguity derives from Article 25(2) DSA, which excludes from its scope all manipulative design choices already covered by the UCPD and GDPR (Sorensen, Sein & Rott, 2023). Article 25(1)'s interaction with the UCPD is the most problematic, while the scope of the GDPR is easier to distinguish, even if there may still be some overlap (Hacker, 2021). This section elaborates on the interplay between these instruments and highlights some grey areas. Other regulations covering dark patterns such as the Consumer Rights Directive or the Unfair Contractual Terms Directive are not considered here, since Article 25(2) DSA does not mention them.

3.2.1 UCPD and GDPR

In general, the interaction between the UCPD and the GDPR is quite clear. First, as *lex specialis*, the GDPR takes precedence in cases of dark patterns related to requests for consent for data processing (Article 3(4) UCPD). Second, the concept of privacy is not mentioned in the UCPD, which excludes it from dealing with violations of consumer's privacy (Hacker, 2021). However, the UCPD does cover one aspect of data protection. Information requirements of the GDPR could be regarded as material information under Article 7(5) UCPD (European Commission, 2021). Therefore, when a platform sells personal data to third parties and derives economic value from this transaction, the gathered data was part of a commercial practice and falls under the scope of the UCPD. Should the trader not disclose that data is being sold to third parties, this could violate Article 7(2) UCPD as a misleading omission of material information. Additionally, it would breach transparency requirements under Article 12 GDPR which could be considered in assessing whether a commercial practice is unfair or not (European Commission, 2021). In such a case the dark pattern could be enforced under both pieces of legislation – under the UCPD as a misleading omission or under the GDPR as a breach of transparency requirements.

3.2.2 DSA and GDPR

The legal scope of the DSA and the GDPR regarding dark patterns is overall clear. The two could seem to overlap when a data controller under the GDPR is simultaneously an online platform under the DSA. In such a situation, the key question is what the dark pattern is for. If it concerns consent to data processing, where users are manipulated to give away more data than they intend to, the GDPR takes precedence. Here, the EDPB's aforementioned guidelines on dark patterns explain in detail which dark patterns constitute practices that induce providing data and are therefore prohibited by the GDPR.

In terms of technical design of an online platform Article 25 DSA can be regarded as complementary to Article 25 GDPR. Both Articles regulate the technical aspects of websites outright rather than prohibiting specific practices. Article 25 GDPR prescribes data controllers to implement data protection by design. They must adopt "appropriate technical and organisational measures" to ensure that the rights of the data subject (such as autonomy) are respected (Article 25(1) GDPR) and that only necessary data is processed (Article 25(2) GDPR). By contrast, Article 25 DSA was framed as a prohibition rather than a principle, but the two Articles complement each other in dark pattern regulation as the GDPR covers all manipulations concerning data gathering, while the DSA (or UCPD) cover all other aspects of manipulative online interface design.

3.2.3 DSA and UCPD

The distinction between the DSA and the UCPD is more difficult to draw. What follows is an exploration of where the limits could be – of what dark patterns fall outside the scope of the UCPD but within that of Article 25 DSA.

Firstly, the subjective scope of the UCPD covers B2C relationships, so its scope would not be met if the commercial practice is not between a trader and a consumer. Conversely, the DSA applies to relationships between online platforms and any sort of user, including business users. Hence, looking at the "manipulating" side, when the dark pattern is implemented by a trader that isn't an online platform, then the design's legality cannot be evaluated using the DSA. This is the case of dark patterns put in place by traders directly on their own websites which they use to sell to consumers. In such instances, the UCPD will still regulate the commercial practices. Nor can Article 25 DSA be used when the party who implements the dark pattern is an online intermediary (subject to the DSA) but not an online platform, as defined in Article 3(i). In such cases, if the intermediary also exceeds the UCPD's definition of a trader engaging in a commercial practice, any potential dark patterns could escape both prohibitions.

From the "manipulated" side, if they are a business or a trader, then this practice will exceed the UCPD's scope but could be prohibited using Article 25 – again, so long as

the “perpetrator” qualifies as an online platform. In practice, though, this interaction between DSA and UCPD is even more complicated, given that some member states such as Austria have transposed the UCPD in a way that extends consumer protection laws to also cover business-to-business (B2B) commercial practices (Civic Consulting, 2011). In contrast, German consumer protection law transposed the UCPD without extending protection to B2B practices (Civic Consulting, 2011), creating an uneven application of the UCPD in various member states.

Focusing on the objective scope of the UCPD, a dark pattern would exceed it either when the commercial practice is not unfair or if the dark pattern is not a commercial practice in the first place. As was mentioned above, the definition of fairness is not clear as it depends on whether fairness is evaluated by the potential or the actual manipulative effect. Furthermore, fairness depends on which recipient standard the deception is measured against. In order to exactly understand the scope the definitional questions must be resolved. Without definitional clarity it is also difficult to ascertain whether a specific practice would be considered unfair under the UCPD or not.

Moreover, whether a practice is commercial is also not straightforward. As mentioned, B2C commercial practices may include acts, omissions or communications before, during or after the sale or supply of a product (Article 2 UCPD). It is unclear whether dark patterns that avoid the platform’s duties under the DSA could be considered a commercial practice. This includes duties such as the notice and action mechanisms (Article 16 DSA), internal complaint-handling mechanisms (Article 20 DSA) and the availability of out-of-court settlements (Article 21 DSA). For example, Article 21 DSA states that platforms must inform users “in a clear and user-friendly interface” that they can take the case before an out-of-court dispute settlement body if users are dissatisfied with the outcome of an appeal. If a dark pattern were implemented to make this process confusing, or to hide complaint-handling mechanisms to avoid users from making use of them, would those practices be considered commercial practices and thus fall under the scope of the UCPD rather than the DSA?

The difficulty in distinguishing whether the DSA or the UCPD applies will have effects on enforcement. In order to be able to apply the DSA, it will first be necessary to establish that a specific dark pattern does not violate the UCPD. This requires clarity on definitions and the scope to be able determine which dark patterns fall outside the objective and the subjective scope of the UCPD and within the scope of the DSA. Especially due to the lack of legal precedent on dark patterns (BEUC, 2022), enforcers could face the issue of not knowing which regulation a dark pattern violates.

3.2.4. A positive: a catch-all as dark patterns evolve

The above subsection drew the conclusion that there is not a clear-cut distinction as to the legal scope of dark patterns covered by the DSA versus those covered by the

UCPD. This is because, from a legal standpoint, the terms of the UCPD have been interpreted so broadly to arguably include most – if not all – the dark patterns that could be found in an online platform (Goanta & Santos, 2023). Additionally, dark pattern prohibition applies to B2B commercial practices in some member states, but not in others as shown by the example of Austria and Germany. This may create confusion in the marketplace as to what applies. Although the unclear interplay between the UCPD and the DSA may cause problems and requires clarification, a potential merit of Article 25 DSA could be functioning as a catch-all for all dark patterns that fall outside the scope of the UCPD as well as future dark patterns.

Considering that manipulative interface designs continuously evolve from being static to more dynamic, new dark patterns may be tweaked slightly to evade existing bans on specific patterns (OECD, 2020, p. 8). With the GDPR it was shown how data processors developed dynamic dark patterns to circumvent the regulatory requirements and frustrate the aim of the regulation (Sinders, 2021). The broad definition of the DSA may reduce the possibility of dark patterns falling through the cracks of regulation by addressing static dark patterns that are not tackled effectively by the existing regulation and covering emerging dynamic manipulations too. If the Commission clarifies the scope to include dynamic manipulations this would additionally support the enforcement of the DSA..

3.3. Enforcement

Overall, the enforcement mechanisms in the EU's legal landscape appear to be well defined within each legal framework. However, the unclearly demarcated scopes of the DSA, the UCPD and the GDPR can lead to uncertainty concerning the right enforcement procedure to endorse in the context of dark patterns prohibitions. On the other hand, the Act might prove effective in increasing the overall oversight efforts of authorities at the European level.

3.3.1. Positive aspects

To this day, enforcement of dark pattern prohibition under the GDPR and UCPD has been insufficient. A study conducted by the European Commission on dark patterns in online commerce websites shows that despite the clear applicability of the UCPD framework, dark patterns proliferate on the Web.

Although Article 25's prohibition does not automatically translate into enforcement, it is noteworthy that from a political perspective, the fact that the DSA is a Regulation with direct effect in all member states (contrarily to a directive like the UCPD which had to be transposed) is something that the Commission could successfully exploit. Under the new framework, the Commission will be able to more directly influence how dark patterns are regulated in the EU, increasing harmonisation in the Union's legal

landscape – both by defining guidelines, and by enforcing cases of dark patterns against VLOPs.

Furthermore, the DSA aims to account for the transnational harmful effects of platform's misbehaviour, by fostering European cooperation between Member States through the creation of a "reliable and secure" information-sharing framework between Digital Services Coordinators (Article 67). In a similar fashion, Article 45 allows member states to communicate with DSCs from different jurisdictions, with the aim to promote uniform EU-wide enforcement. This mechanism represents a safeguard against heterogeneous enforcement that could otherwise arise due to infrastructural differences in the digital domain characterising different member states. In this regard, the DSA aims to avoid perpetuating the pitfalls of the UCPD's enforcement. It is noteworthy how Articles 58 and 60 DSA are also aimed at promoting coordination between the Commission, the European Digital Services Board and the DSC, for instance by allowing the joint investigation of Coordinators or joint regulatory requests to Member States to come from both the Board and the Coordinators.

There is also the fact that illicit practices concerning dark patterns are going to be quite context- and even service-specific. By entitling itself with the power to produce Guidelines on dark patterns, the European Commission is making it likelier that the development of these provisions will stay within its control; that it will more closely follow the Commission's preferred view of the matter. This is because Commission Guidelines have an authoritative effect; businesses often use them as guides for best practices and other authorities also base upon them their application of the law (Terpan 2014).

Furthermore, the inclusion of an additional prohibition on dark patterns means that there is going to be a higher degree of regulatory oversight on potential dark patterns. In this sense, it is notable that the DSA's enforcement provisions provide for the creation of national Digital Services Coordinators (DSCs) and a European Digital Services Board. These DSCs need not be new institutions. In fact, all the countries who as of date have announced their DSCs have appointed a pre-existing authority (Ledger, 2023). Nevertheless, the creation of DSCs does mean that an authority that was not responsible for dark patterns monitoring before, is now empowered to do so – such is the case in Ireland and Hungary, where the national media regulators have been appointed as DSCs. In other cases, it means that an authority that was already regulating dark patterns now disposes of another legal instrument to effectively regulate them. This is for instance, going to be the case in the Netherlands, where the consumer authority, in charge of implementing the UCPD[6], has also been appointed DSC. Hence, the same authority is empowered to act against dark patterns through two different legal frameworks.

An additional point that may improve enforcement is the applicability of the DSA to intermediaries based outside of the Union. Under the UCPD, the application of dark patterns to foreign traders was subject to the traditional – and more time-consuming – mechanisms of private international law (European Commission, 2021, p. 25). By contrast, the DSA, mirroring the GDPR, sets to regulate online intermediaries regardless of their place of establishment, so long as their services are accessible in the EU. To achieve this, the DSA conditions continued access to the Single Market to the appointment of a legal representative in the EU, who must have the necessary powers and resources to guarantee effective compliance with the DSA (Article 13 DSA). In this sense, even though the UCPD can apply to traders established in third countries, the DSA's terms may make it easier to effectively enforce a prohibition on dark patterns.

3.3.2. Negative aspects

The fragmentation in legal instruments dealing with dark patterns in online platforms may create uncertainty not only concerning which regulations apply, but also about which authority should exert enforcement. In this context, the interaction between the UCPD and the DSA may create tension between DSCs and regulators at national level in terms of effective enforcement. Practically speaking, different national authorities have different relative influence. Hence, the same concept of dark pattern may end up being enforced by different authorities using a different legal basis (UCPD or DSA) depending on the amount of resources at their disposal, and the consequent relative power of one body on the other.

Thus, although the DSA defines the creation of coordination mechanisms between the Digital Services Coordinators, it does not account for the coordination of these with consumer protection bodies that aim to tackle the same issues. This represents a significant pitfall, especially when considering the lack of clarity concerning the scope of the DSA and the UCPD. In this context, communication failures between Digital Services Coordinators and consumer protection authorities, might lead to problematic double liability issues where platforms get investigated and fined both under the UCPD and the DSA for the same infringement, as well as to ineffective enforcement procedures.

Much like the issues about legal scope, uncertainties about enforcement affect not only the enforcing authority (or authorities), but also the players in the market. Uncertainties about what applies, who enforces, and how to comply can greatly hinder the ability of market participants to organise their activities and understand their obligations.

3.4. The DSA toolbox: More tools for tackling dark patterns

Finally, enforcement authorities and the Commission in particular can consider how other DSA provisions, outside of Article 25, can be used to prevent the diffusion of misleading interfaces. A holistic reading of the DSA reveals the following opportunities:

3.4.1. Duties for very large online platforms (VLOPs)

The DSA's tiered approach views size as an indicator of risk and imposes asymmetrical obligations depending on size. VLOPs, or online platforms with over 45 million monthly average users in the EU (Article 33 DSA), have additional duties that aim to tackle the greater risks associated with their platforms. Some VLOP-specific obligations can impact the use of confusing design interfaces. Here, the Commission will have a key role to play, as the main enforcer of the DSA *vis a vis* VLOPs and very large online search engines (VLOSEs).

For instance, VLOPs' duty to assess systemic risks (Article 34) may be used to compel them to determine the potentially negative impacts of design choices that, although perhaps fail to be "dark" enough to be illegal patterns under Article 25 DSA, may nevertheless confuse recipients. In this sense, VLOPs must assess their service's actual or foreseeable impact on the exercise of fundamental rights, including human dignity, data protection, children's rights, and consumer protection. Risks to children's rights may arise from "the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors" (Recital 81). Whereas risks to public health and individuals' wellbeing may similarly arise from "online interface design that stimulates behavioural addictions" (Recital 83).

Following risk identification, VLOPs must mitigate them with measures that will be evaluated by the Commission (Article 35). Recital 87 DSA explicitly states that adapting an interface can be an appropriate mitigation measure. Together, these articles provide encouragement for VLOPs to implement more neutral interfaces and mitigate the potentially negative impacts of design choices that, although perhaps not misleading enough to breach Article 25, may nevertheless confuse recipients, exploit children's weaknesses, or stimulate addictive behaviours. The Commission can therefore look at employing this provision as a *positive* incentive to choose neutral interfaces. Here, the focus is taken away from costly legal determinations of whether a design element crosses the line of illegality – concentrating instead on the risks and harms that can be avoided through opting for neutral choices.

Finally, researchers' role under the DSA may also enable better policy making over dark patterns. As Luguri & Strahilevitz (2021) note, there is a vacuum in publicly-available research on dark patterns' effectiveness at actually deceiving users. This research has mainly taken place behind closed doors, within companies, using the data that only they can access. Yet Article 40 DSA provides a framework for compelling VLOPs to give data access to vetted researchers. Of course, research access will have

limits, as VLOPs have a legitimate right to keep sensitive information, like trade secrets, private. Nevertheless, their work could provide new insights, enabling better regulation and enforcement.

3.4.2. Other

Dark patterns may affect other DSA duties that apply to all sorts of online intermediaries, beyond online platforms. For instance, Article 14 DSA mandates that all online intermediaries publish intelligible and accessible terms and conditions, including information on any content moderation policies. Dark patterns that hide or muddle terms and conditions could contradict this duty. Furthermore, Article 16 DSA dictates that hosting service providers[7] must have notice and action mechanisms for any user to notify illegal content. This mechanism must be easy to access and user friendly. Hence, if the intermediary uses design elements to hide it or to make it burdensome to use, such a dark pattern would arguably breach Article 16 DSA.

4.4. Conclusions and recommendations

Despite multiple regulatory efforts, dark patterns remain a prevalent element of EU citizens' experiences online, hampering their ability to autonomously define and act upon their preferences. In this challenging context, the Digital Services Act adds a new dimension. This policy brief has analysed the DSA's approach to dark patterns, focusing on Article 25's prohibition on dark patterns. Following a summary of the EU legal framework on dark patterns and an analysis of Article 25, this brief has highlighted four areas that the European Commission must address in order to best implement the new prohibition. Here, implementation is understood as optimal if it contributes to a consistent and effective legal framework for tackling dark patterns. We therefore call upon the EC to act on its powers to produce guidelines on Article 25, taking into account the following recommendations.

4.1. Clarify terms

Section 3.1 outlined three main definitional uncertainties within Article 25 that could hamper its effectiveness: (i) whether the prohibition extends to manipulative interface personalisation, (ii) whether the manipulative effect must be actual or potential, and (iii) whether the standard used to determine said effect is the "average consumer" standard. The Commission should take the opportunity to clarify these points in the following manner.

4.1.1. Manipulative interface personalisation would be better addressed by strengthening data protections under the GDPR

Despite their potential inclusion under the DSA prohibition, it is not necessarily true that manipulative interface personalisation is best addressed as a dark pattern. The EC's 2022 report on this subject is instructive: it claims that "businesses are making increased use of personalisation practices and combining them with dark patterns", but simultaneously reveals that its investigation "did not identify significant cases of manipulative personalisation" (p. 6). The nature of information asymmetry, algorithmic opacity, and the general challenge of identifying problematic personalisation where it occurs has prevented the UCPD from adequately confronting this issue. We can expect that it would be an equivalent challenge under the DSA.

It is for this reason that manipulative interface personalisation would be better addressed at its source (i.e. personal data supply), rather than in its outward (often un-) observable materialisation. As the EC acknowledges, these types of practices "fall at the intersection of consumer protection, data protection, and other relevant instruments in the EU legal framework" (2022, p. 7). Manipulative interface personalisation is based on the collection and processing of data to reveal information about an individual user that can be operationalised to promote actions favourable to the data controller. A prohibition against these practices could be considered within the context of Article 9 of the GDPR, which prohibits the processing of several categories of personal data "for the purpose of uniquely identifying a natural person." This Article, however, is currently ill-equipped to reduce the data supply that underpins manipulative interface design as it limits its focus to specific categories of particularly sensitive personal data (e.g. biometric data, race, and religion) and exempts circumstances where the data subject's explicit consent to processing is provided. This is problematic as manipulative interface personalisation can be based on categories of data that are not subject to the Article 9 restrictions and consent, where provided, can be corrupted by manipulative interface personalisation in and of itself.

The EC should consider whether the broader practice of manipulative interface personalisation aligns with the GDPR's general stated aim to ensure… "personal data (is)… collected for specified, explicit and legitimate purposes" (GDPR(5)(1)(a)). As the EC's 2022 study emphasised, this discussion ultimately rests on differentiating "legitimate" personalisation from manipulative personalisation. Of course, there are circumstances under which personalisation is beneficial for users; it can legitimately aid users to navigate the vast cacophony of online life more efficiently and productively. However, we believe that manipulative interface personalisation is a pervasive and growing problem that cannot be adequately addressed by prohibiting its observable manifestation given it is rarely observable or detectable from the "outside", as we have established. Regulatory action must thereby focus on cutting the data supply that fuels these practices, while taking care to allow for legitimate personalisation practices where possible. We believe that the GDPR's core purpose and remit is best positioned to pursue this regulatory agenda, not Article 25 of the DSA.

4.1.2. Accept a potential effect

Article 25 DSA does not clarify whether the effect of deceiving the user needs to be actual or if a potential effect may suffice. To better meet the DSA's objectives of protecting users' rights and creating a trustworthy environment (recital 12), the provision should encompass both. This conclusion is further supported by the fact that the UCPD only requires a likely effect to deceive. Given that dark patterns remain so prevalent despite the pre-existing legal framework being "lenient" in this way, and given that Article 25 DSA aims to catch dark patterns that exceed the UCPD's scope, setting a higher threshold in Article 25 would frustrate the policy objective.

4.1.3. Lower the recipient standard

The European Commission should clarify what recipient standard will be used to determine whether a pattern is likely to deceive users. Here, to better protect users' rights and reflect the power asymmetries described above, Article 25 DSA should be implemented using a lower standard than the "average consumer" benchmark typical of the UCPD.

The lack of complementarity between the UCPD's and the DSA's standards could lead to some less desirable consequences, particularly in practical enforcement terms: the same dark pattern could be deemed illegal if assessed by one country's DSC, and legal if analysed by the consumer protection authority. However, in a way this matches Article 25's purpose of capturing online interfaces that exceed the pre-existing framework. Furthermore, given that consumer law itself is moving towards a recognition of the inherent vulnerabilities in dark patterns (read footnote 5), if the DSA adopts this lower threshold, the desire for complementarity between UCPD and DSA (especially because of the need by market actors of legal certainty) might give the final push needed to fully change the standard in consumer law, too; better aligning it with the digital age.

4.2. Clarify scope

The European Commission should provide legal clarity on the scopes of the GDPR, UCPD and the DSA regarding dark pattern regulation. Currently, the interplay between legislation on dark patterns could lead to ineffective regulation. Therefore, the Commission should address the unclear application of the UCPD by elaborating on the subjective and objective scope of the Directive. Specifically, the interaction of the DSA with the different transpositions of consumer protection law needs clarification, considering that some Member States extend prohibitions of manipulative practices to B2B commercial practices. Furthermore, this policy brief has given specific examples of particular practices that perhaps exceed the UCPD's scope and could therefore be included within the scope of Article 25 – such as hiding complaint handling mechanisms. The Commission should provide guidance on where these practices fall..

4.3 Coordinate enforcement

The European Commission should clearly delineate a framework for the coordination between national consumer protection authorities, responsible for UCPD's enforcement, and national Digital Services Coordinators. This can be done by setting a clear procedural communication mechanism. For instance, it can be complemented with Article 45 or Article 67 DSA and prescribe the mandatory notification of investigation launches as well as of fine impositions to the respective authorities. Such a solution would at least avoid any risk of double liability instances, and would increase the clarity of the regulatory framework also with regards to the scope. In this sense, the recommendation would increase the alignment of the DSA with two of the three main objectives of this policy brief, namely with ensuring a *consistent EU legal framework* on dark patterns and procuring its *effective enforcement*.

4.4. Harness the full DSA toolbox

The Commission should explore how other DSA provisions may be used to tackle the use of deceptive online interfaces, both by online platforms and by other online intermediaries. As highlighted in Section 3.4, a transversal reading of the DSA from the perspective of dark patterns reveals many opportunities, ranging from systemic risk assessments by VLOPs to the accessibility of notice & action mechanisms by all hosting service providers.

One of the most promising opportunities relates to giving data access to vetted researchers. As mentioned, Article's framework could enable researchers to provide new insights on dark patterns, especially as they continue to evolve, enabling better regulation. Yet the Commission must keep in mind the ways in which intermediaries may try to circumvent giving meaningful access: whether misusing legitimate interest claims, or providing researchers with data dumps that are impossible to analyse, instead of the structured data that the company uses to design and test interfaces. What matters is not only the fact of giving access, but also the conditions of this access. In this sense, to channel Article 40's potential vis a vis dark patterns, the Commission must ensure that researchers are given meaningful access while respecting all legitimate interests.

Beyond this specific case, the insights outlined in Section 3.4 can provide reassurance to those who worry that the Article 25 prohibition should have been expanded to cover other online intermediaries (e.g. Lomas, 2022) – there are tools within the DSA to expand the oversight of dark patterns beyond the subjective scope of Article 25 (i.e. online platforms). There are also ways to positively encourage more neutral interfaces, beyond a strict prohibition like Article 25. This sort of creative policy-making could

perhaps be a missing piece of the puzzle in successfully curbing the proliferation of dark patterns in the EU.

5.5. References

Legislation

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 ELI: http://data.europa.eu/eli/treaty/char_2012/oj

Consolidated Version of the Treaty on European Union [2008] OJ C115/13

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')* OJ L 149/22 ELI: http://data.europa.eu/eli/dir/2005/29/oj

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence *('Artificial Intelligence Act')* and amending certain Union legislative acts [2021] COM/2021/206

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 L 119/1 ELI: http://data.europa.eu/eli/reg/2016/679/2016-05-04

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 L 265/1 ELI: http://data.europa.eu/eli/reg/2022/1925/oj

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 L 277/1 ELI: http://data.europa.eu/eli/reg/2022/2065/oj

Case law

European Court of Justice, Judgement of 1 October 2019, *Planet49 GmbH,* C-673/17, ECLI:EU:C:2019:801

European Court of Justice, Judgement of 11 November 2020, *Orange Romania,* C-61/19, ECLI:EU:C:2020:901

European Court of Justice, Judgement of 16 July 1998, *Gut Springenheide and Tusky*, C-210/96, ECLI:EU:C:1998:369

Dutch Trade and Industry Appeals Tribunal, Judgement of 15 May 2018, *ACM/Corendon*, Case 17/1179, ECLI:NL:CBB:2018:145

Other

ACM (2022). *Guidelines on the protection of the online consumer: Boundaries of online persuasion.* Dutch Authority for Consumers and Markets. https://www.acm.nl/en/publications/guidelines-protection-online-consumer

BEUC (2022, February 7). *"Dark patterns" and the EU consumer law acquis*. Recommendations for better enforcement and reform. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf

Cauffman, C., & Goanta, C. (2021). A new order: the digital services act and consumer protection. *European Journal of Risk Regulation*, *12*(4), 758-774.

Civic Consulting. (2011). *Study on the application of Directive 2005/29/EC on unfair commercial practices in the EU.* European Commission. https://op.europa.eu/en/publication-detail/-/publication/5550d564-65af-47c8-b7e4-a44020ad4a78

Ecommerce Europe. (2022, June 14). *Ecommerce Europe's reply to the Call for evidence on Digital fairness*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/F3296360_en

EDPB. (2022).*Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them.* https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

European Commission. (2020, December 15). *Commission staff working document impact assessment.* Impact Assessment of the Digital Services Act. https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act

European Commission. (2021). 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. *Official Journal of the European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)

European Commission (2023, January 30). *Consumer protection: manipulative online practices found on 148 out of 399 online shops screened*. https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418https:/op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418

European Commission. (2022). *European declaration on digital rights and principles for the digital decade.* https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration

Goanta, C., & Santos, C. (2023). Dark Patterns Everything: An Update on a Regulatory Global Movement. *Network Law Review*.

Gumbis, J., Bacianskaite, V., & Randakeviciute, J. (2008). Do human rights guarantee autonomy?. *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, (62), 77-93.

Hacker, P. (2021). Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. *European Law Journal*.

Helberger, N., Sax, M., Strycharz, J., & Micklitz, H.-W. (2021). Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. *Journal of Consumer Policy,* 45, 175-200. https://doi.org/10.1007/s10603-021-09500-5

Lomas, N. (2022, April 13). EU's digital rule-book reboot could fumble dark patterns ban and trader checks, warns BEUC. TechCrunch. https://techcrunch.com/2022/04/13/dsa-beuc/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAG6LGvNEjYYiDr3CBjxmlRCRpLmLVEQDViZEH3RP05Cc3NrT7yHkCd46AVlnJhKb_M-veL0jzuZA29gKHSldIjaC8DTWxOxBIq92blcLismOcwTkmLwuxnXCyYbweyX0gHakPjbbnOQoVpUyY71EESj6nTP2FXHOgH_WPaOL0Q2_

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

Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., Rodríguez de las Heras Ballell, T. (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*. European Commission. https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418

OECD. (2020). *Roundtable on dark commercial patterns online. Summary of discussion.* https://one.oecd.org/document/DSTI/CP(2020)23/FINAL/En/pdf

Sinders, C. (2021). *Designing against dark patterns*. *German Marshall Fund of the United States.* https://www.jstor.org/stable/pdf/resrep33487.pdf

Sorensen, M. J., Sein, K., & Rott, P. (2023). *Response of the European Law Institute*. European Law Institute. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_to_the_European_Commission_s_Public_Consultation_on_Digital_Fairness_.pdf

Terpan, F. (2015). Soft law in the European Union: The changing nature of EU law. *European Law Journal*, *21*(1), 68-96.

---

[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.

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

[3] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

[5] The UCPD Guidelines recognise that that “multi-dimensional forms of vulnerability are particularly acute in the digital environment” (European Commission, 2021, p. 35) and that, regarding dark patterns, “the benchmark of an average or vulnerable consumer can be modulated to the target group [of the practice], even formulated from the perspective of a single person who was subject to the specific personalisation” (*ibid.*, p. 100).

[6] And, in fact, one of the most active in policy-making regarding commercial dark patterns. The Dutch Consumer Authority (ACM) published a very comprehensive guidance for traders on how it evaluates dark patterns under the UCPD – more accurately, under the national transposing law. See ACM, 2022.

[7] That is, intermediaries that host user-generated content (Article 3(g)(iii)), whether or not they disseminate it publicly. If they do, then they are an online platform.

About the authors :

Tom Akhurst: Sciences Po Master in Public Policy, Digital, New Technology and Public Policy stream; Bachelor of Arts graduate, University of Melbourne; first class honours thesis on China's 'Digital Silk Road'; former speechwriter to a minister in the Australian Government; former research scholar at Blueprint Institute.

Laura Zurdo: Master in Public Policy, Digital, New Technology & Public Policy stream; Law and International Relations Graduate, Universidad Pontificia de Comillas - ICADE; European digital platform regulation; Policy Analyst at Tremau.

Riccardo Rapparini: Master in Public Policy - Digital, New Technology and Public Policy stream; BSc in Philosophy, Politics and Economics (PPE), Vrije Universiteit Amsterdam; External Consultant at OECD AI Policy Observatory.

Christoph Mautner Markhof: Master in Public Policy: Digital, New Technologies and Public Policy stream; Politics, Psychology, Law and Economics (PPLE), University of Amsterdam; Majored in Politics.

About the Digital, governance and sovereignty Chair:

Sciences Po's Digital, Governance and Sovereignty Chair's mission is to foster a unique forum bringing together technical companies, academia, policymakers, civil societies stakeholders, public policy incubators as well as digital regulation experts. Hosted by the School of Public Affairs, the Chair adopts a multidisciplinary and holistic approach to research and analyse the economic, legal, social and institutional transformations brought by digital innovation. The Digital, Governance and Sovereignty Chair is chaired by **Florence G'sell**, Professor of Law at the Université de Lorraine, lecturer at the Sciences Po School of Public Affairs.

The Chair's activities are supported by: