

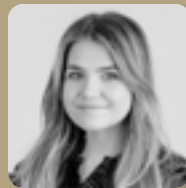
# DARK PATTERNS – A EUROPEAN REGULATORY PERSPECTIVE



**BY  
KATRINA  
ANDERSON**



**&  
NICK  
JOHNSON**



**&  
AMELIA  
HODDER**

Katrina Anderson is an associate director, Nick Johnson, a partner, and Amelia Hodder, a trainee solicitor, at Osborne Clarke, an international legal practice headquartered in London.

### **DRAWING LINES AROUND DARK PATTERNS**

By Maneesha Mithal & Stacy Okoro



### **LOOKING BEYOND THE PRIVACY POLICY: REGULATORY SCRUTINY OF DARK PATTERNS IN USER INTERFACES**

By Christine Chong & Christine Lyon



### **DARK PATTERNS - A EUROPEAN REGULATORY PERSPECTIVE**

By Katrina Anderson & Nick Johnson



### **DARK PATTERNS DEFINED: EXAMINING FTC ENFORCEMENT AND DEVELOPING BEST PRACTICES**

By Ryan C. Smith



### **DARK PATTERNS: PROTECTING CONSUMERS WITHOUT HINDERING INNOVATION**

By Victoria de Posson



### **DARK PATTERNS AND MANIPULATION**

By Marcela Mattiuzzo



### **UNCLOAKING DARK PATTERNS: IDENTIFYING, AVOIDING, AND MINIMIZING LEGAL RISK**

By Kyle R. Dull & Julia B. Jacobson



### **TACKLING DARK PATTERNS: HOW TO REASONABLY PREVENT CONSUMER MANIPULATION AND COMPETITION DISTORTIONS?**

By Frédéric Marty & Jeanne Torregrossa



Visit [www.competitionpolicyinternational.com](http://www.competitionpolicyinternational.com)  
for access to these articles and more!

### **DARK PATTERNS - A EUROPEAN REGULATORY PERSPECTIVE**

By Katrina Anderson & Nick Johnson

Dark Patterns are deceptive and manipulative features of a user interface that push or nudge consumers into making certain choices that are not in their best interests. Such features are increasingly catching the eye of consumer and data protection regulators across Europe, including in the UK, the EU and beyond. However, considerable uncertainty remains over their legality and indeed their definition itself. The EU's Unfair Commercial Practices Directive ("UCPD") at an EU level, and Consumer Protection from Unfair Trading Regulations 2008 ("CPUT") in the UK are increasingly being used by have allowed regulators to begin to challenge the fairness of the application of dark patterns. Dark patterns have similarly challenged on the basis they been shown to undermine some of the principles of the General Data Protection Regulations ("GDPR"). However, the law continues to be difficult to apply in the absence of practical guidance or a body of case law. The question therefore remains over when a dark pattern will cross the threshold from divisive marketing technique to illegal practice. With new legislation expressly outlawing dark patterns [notably the EU Digital Services Act and the EU Data Act,] on its way, will this provide more clarity on where the legal lines are drawn?

**Scan to Stay Connected!**

Scan here to subscribe to CPI's  
**FREE** daily newsletter.



# 01

## INTRODUCTION TO DARK PATTERNS

Dark patterns is a term that refers to deceptive and manipulative features of a user interface ("UI") that push or nudge people into making choices that are not in their best interests. While concern about dark patterns is growing amongst European consumer and data protection regulators, there is still considerable uncertainty over when the use of dark patterns will cross the threshold from persuasive marketing technique to illegal practice.

As the e-commerce world has become more sophisticated, businesses have developed more and more innovative methods to influence consumer choices, culminating in a perception that there is a culture of "dark pattern" usage. Regulators in Europe typically take the view that consumers encountering dark patterns on retailer websites may end up, for example, purchasing items more quickly and with less consideration than intended, or entering into subscriptions and being unable to cancel them. Data protection regulators are concerned that dark patterns may coax users into inadvertently consenting to the processing of their personal data or accepting more privacy-intrusive settings than they otherwise might.

Despite being a major concern for European regulators, dark patterns did not start as a legal concept and as a result they are not clearly or consistently defined. For example, the newly enacted EU Digital Services Act (the "DSA")<sup>2</sup> refers to them as practices on the UI that "materially distort or impair, either

on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions."<sup>3</sup> Similarly the EU's proposal for the Data Act<sup>4</sup> views dark patterns as "design techniques that push or deceive consumers into decisions that have negative consequences for them."<sup>5</sup> In subtle contrast, the guidelines of the European Data Protection Board (the "EDPB") on dark patterns in social media platform interfaces<sup>6</sup> consider dark patterns themselves to be a form of UI or user experience<sup>7</sup> and deem the decisions that users are pushed into regarding their personal data to be "unintended, unwilling and potentially harmful."<sup>8</sup>

Adding further uncertainty are the multiple typologies of dark pattern and variations in their names. Recently, the UK's Consumer and Markets Authority (the "CMA") flagged 21 potentially harmful forms of "Online Choice Architecture" (which is the term the CMA and Dutch regulator<sup>9</sup> use for dark patterns) practice, divided into three categories; those affecting choice structure (the design and presentation of options), choice information (the content and framing of information provided), and choice pressure (through indirect influence of choices).<sup>10</sup> It has pinpointed the dark patterns it considers "almost always harmful" as "choice overload and decoys," "sensory manipulation," "sludge," "dark nudge," "forced outcomes," "drip pricing," "complex language," and "information overload."<sup>11</sup>

In January this year the European Commission announced the results of a sweep by the Consumer Protection Cooperation (the "CPC") of 399 retail websites which showed that nearly 40 percent were using "manipulative online practices to exploit consumer vulnerabilities or trick them."<sup>12</sup> The sweep focused on the following dark patterns: fake countdown timers; web interfaces designed to lead consumers to purchases, subscriptions or other choices; and hidden information.

---

2 European Council Regulation No. 2022/2065, 2022 O.J (L 277/1) (Digital Services Act).

3 *Ibid.* at Recital 67.

4 Proposal for European Council Regulation on harmonised rules on fair access to and use of data No. 2022/0047(COD), 2022 COM(2022) 68 final (Data Act Proposal).

5 *Ibid.* at Recital 34.

6 European Data Protection Board, Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, 3/2022 1. (March 14, 2022). [https://edpb.europa.eu/system/files/2022-03/edpb\\_03-2022\\_guidelines\\_on\\_dark\\_patterns\\_in\\_social\\_media\\_platform\\_interfaces\\_en.pdf](https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf).

7 *Ibid.* at page 7.

8 *Ibid.*

9 Netherlands Authority for Consumers and Markets (ACM).

10 Competition and Markets Authority, Discussion Paper, *Online Choice Architecture: How digital design can harm competition and consumers*, CMA155 (April 2022). [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1066524/Online\\_choice\\_architecture\\_discussion\\_paper.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf).

11 *Ibid.*

12 Press Release, European Commission, Consumer protection: manipulative online practices found on 148 out of 399 online shops screened (Jan. 30, 2023), (IP/23/418) [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_418](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418).

Our review of the different typologies and naming conventions suggests that while there is a lack of consensus about the names of the different dark patterns themselves, dark patterns can broadly be broken down into nine themes:

1. Pressure – repeatedly being asked to act or confronted with (alleged) social norms or scarcity of goods.
2. Force – users are (*de facto*) forced to take action or acquiesce to do something.
3. Obstacles – users face various obstacles to dissuade them from taking certain actions.
4. Sneaking – additional purchases or goods or services are imposed on users.
5. Deception and misdirection – the UI is created to distract from relevant information or to frustrate the usual expectations of the UI design.
6. Overloading – users are faced with an avalanche of requests, information, options or possibilities in order to prompt them to make certain choices.
7. Hindering – the obstruction or blocking of users from becoming informed or being able to make certain choices.
8. Fickle – UI design that is inconsistent or not clear, making it hard for the user to navigate to make the choices they want to make.
9. Left in the dark – UI designed to hide information or choices.

We consider that individual dark patterns can then be categorized within these themes. For example, confirm-shaming (where the UI attempts to make the user feel guilty for selecting their preferred option) and limited stock notifications sit within "Pressure." "Roach motels" (subscription traps with numerous barriers to cancel, making cancellation significantly harder than signing up) would come under "Obstacles."

Currently "roach motels," pre-selection of advantageous choices and false timers seem to be drawing particular attention in Europe.

# 02

## REGULATION OF DARK PATTERNS

The concept of reducing friction and optimizing UI design has been around for many years. Even the idea that consumers might be "nudged" into certain choices is not new. Consumer protection and data protection law have always applied to UI design as much as to other aspects of businesses' interactions with consumers. However, it is only recently that European regulators and legislators have used the term "dark patterns" and specifically called out how consumer protection and data protection law should regulate these practices.

Increasingly dark patterns are explicitly mentioned and expressly outlawed in new and proposed legislation, such as in the DSA.<sup>13</sup> Further, the EU's public consultation as part of the Fitness Check of EU consumer law on digital fairness<sup>14</sup> clearly had dark patterns in mind when it probed respondents on whether: they had experienced websites designed to pressure them to purchase and make them uncertain of their rights and obligations; they had encountered difficulties cancelling subscriptions; and they would agree that stronger protections against "digital practices that unfairly influence consumer decision-making"<sup>15</sup> were required.

### A. Consumer Law

The use of dark patterns can contravene the Unfair Commercial Practices Directive<sup>16</sup> (the "UCPD") at an EU level, which is mirrored in the UK by Consumer Protection from Unfair Trading Regulations 2008 ("CPUT").<sup>17</sup> These prohibit unfair commercial practices, including practices that amount to misleading actions or omissions, that are aggressive or that use harassment, coercion or undue influence. A commercial practice is also unfair under this legislation if it is "contrary to the requirements of professional diligence"<sup>18</sup> and "it materially distorts or is likely to materially distort the economic behavior with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is

---

13 Digital Services Act, *supra* note 2, at Article 25.

14 European Commission, Consultation, *Digital fairness – fitness check on EU consumer law* [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/public-consultation\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/public-consultation_en).

15 *Ibid.*

16 European Council Directive No. 2005/29, 2005 O.J (L 149/22).

17 The Consumer Protection from Unfair Trading Regulations 2008, SI No. 2008/1277.

18 Unfair Commercial Practices Directive, *supra* note 16 at Article 3(2)(a).

directed to a particular group of consumers."<sup>19</sup> Guidance on the UCPD from the European Commission<sup>20</sup> expressly states that it can be utilized to challenge the fairness of the application of dark patterns in business-to-consumer commercial relationships and suggests, for example, that confirm-shaming could amount to an "aggressive practice using undue influence to impair the consumer's decision-making."<sup>21</sup> It also sets out the practices often recognized as dark patterns that are caught by the list of so-called "blacklisted offences" – commercial practices that are always considered unfair under the UCPD (which is also replicated in CPUT).

The "blacklisted offences" under the UCPD and CPUT include, for example, "[f]alsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice."<sup>22</sup> It is easy to see how the use of countdown timers, a "Pressure" dark pattern, could fit within this if they are counting down to the expiry of a sale or deal which will not in fact end when the timer ends and are therefore false. This is endorsed by the European Commission's guidance on the UCPD<sup>23</sup> and the CMA also took this view when it announced at the end of 2022 that it would be examining whether the mattress-in-a-box company, Emma Sleep, had misled consumers by using countdown timers that implied a discount would end, when this was potentially not the case.<sup>24</sup> This investigation by the CMA forms part of its Online Choice Architecture program to tackle potentially harmful online selling practices.

Even if the practices targeted are not always expressly referred to as "dark patterns," there has been significant enforcement across Europe under consumer protection legislation. An early example of regulation of dark patterns under

the UCPD is the Italian Competition Authority's ("AGCM") decision to fine two online travel operators for using practices that hindered consumers' ability to view all of the relevant information on additional costs attached to the purchase.<sup>25</sup> It also found the automatic pre-selection of an optional insurance policy misled consumers into believing this was compulsory. The AGCM in general has been active in its use of consumer law to regulate dark patterns. More recently, the Norwegian Consumer Council has written to various platform hosts alleging the use of dark patterns in their interfaces.

---

**“Even if the practices targeted are not always expressly referred to as "dark patterns," there has been significant enforcement across Europe under consumer protection legislation**

---

Further, The CPC's sweep of dark patterns in relation to e-commerce and the call for European consumer protection regulators to contact e-commerce websites which have been identified as featuring dark patterns<sup>26</sup> may very well lead to enforcement. The CMA also announced that the *Emma Sleep* investigation would be the first of its investigations in relation to Online Choice Architecture<sup>27</sup> and therefore further action is anticipated in the UK in the coming months.

## **B. Data Protection Law**

The "fair processing" principle in Article 5(1)(a) of the General Data Protection Regulation ("GDPR")<sup>28</sup> requires that data be

---

19 *Ibid.* at Article 3(2)(b).

20 European Commission, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, 2021 O.J. (C 526/1) (Guidance on the Unfair Commercial Practices Directive).

21 *Ibid.* at 4.2.7.

22 Unfair Commercial Practices Directive, *supra* note 16 at Annex 1 and The Consumer Protection from Unfair Trading Regulations, *supra* note 17 at Schedule 1 .

23 Guidance on the Unfair Commercial Practices Directive, *supra* note 20 at 4.2.7.

24 Press Release, Competitions & Markets Authority, CMA investigates online selling practices based on 'urgency' claims (November 30, 2022) <https://www.gov.uk/government/news/cma-investigates-online-selling-practices-based-on-urgency-claims>.

25 Press Release, Italian Competition Authority, PS7488-PS7245 - Air transport: Antitrust fines Ryanair and EasyJet for more than a million euro due to misleading practices in the travel insurance (February 17, 2014) <https://en.agcm.it/en/media/press-releases/2014/2/alias-2105>.

26 [https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps\\_en#:~:text=2022%20%E2%80%93%20sweep%20on%20dark%20patterns,-Manipulative%20practices%20called&text=The%20CPC%20authorities%20decided%20to,products%20for%20their%20own%20account](https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#:~:text=2022%20%E2%80%93%20sweep%20on%20dark%20patterns,-Manipulative%20practices%20called&text=The%20CPC%20authorities%20decided%20to,products%20for%20their%20own%20account).

27 CMA investigates online selling practices based on 'urgency' claims, *supra* note 24.

28 European Commission Regulation No. 2016/679, 2016 O.J. (L119) (GDPR).



processed "fairly and in a transparent manner."<sup>29</sup> The EDPB has also stated that "fairness is an overarching principle which requires that personal data shall not be processed in a way that is unjustifiably detrimental, discriminatory, unexpected or misleading to the data subject."<sup>30</sup> Arguably, therefore, if a UI uses dark patterns to facilitate insufficient or misleading information in respect of the processing of data for the user, this will necessarily amount to unfair processing. Additionally, where consent is the lawful basis for the processing of personal data, the GDPR requires this to be "given freely, informed and unambiguous"<sup>31</sup>. Dark patterns employed to push users to agree to give away more personal data than necessary (such as nagging and continuous prompting – forms of "Pressure" dark pattern) may render such consent invalid.

Article 25 of the GDPR additionally imposes an obligation on data controllers to practice data protection by design and default.<sup>32</sup> EDPB guidance explains that the fairness elements of design and default include an absence of deception, specifically "[d]ata processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design."<sup>33</sup> It is again likely that using dark patterns, such as a false hierarchy (for example a green "reject" button and red "accept" button) or confirm-shaming, could undermine the Article 25 requirements.

Enforcement action has already been taken under the GDPR to regulate dark patterns. For example, the Court of Justice of the European Union held that the automatic pre-selection of checkboxes, a form of "Obstacles" dark pattern, by an online lottery service did not provide valid consent for the use of cookies or similar technologies.<sup>34</sup> This practice was held to be in breach of the GDPR as consent was not freely given.

Recent guidance by the EDPB on dark patterns in social media platform interfaces<sup>35</sup> is another example of the increased attention in this area on the part of regulators, and sheds some further light on the relationship between use of dark patterns and GDPR compliance. It calls for national regulators to sanction dark patterns that breach the GDPR and provides examples of best practice for various parts of the social media interface in contrast to illustrations of

potentially illegal use of dark patterns. While the guidelines focus on social media platforms – a perennial target of European data protection regulators – its principles would generally seem to be equally applicable to other online UIs.

## 03

### WHEN ARE DARK PATTERNS UNLAWFUL? – A LACK OF CERTAINTY UNDER THE LAW

As the concept crystalizes, it is becoming easier to understand which features of the UI raise concerns and might amount to a dark pattern. However, what remains less clear is exactly when a dark pattern will cross the line into being unlawful. There is now no doubt that dark patterns *can* amount to a breach of consumer and data protection laws, but the grey area over when exactly this threshold is crossed is problematic for businesses seeking to achieve compliance.

#### *A. Principles-Based Laws and an Absence of Clear Guidance and Case Law*

The issue legally is that Europe's principles-based consumer protection and privacy laws are only lightly tested in relation to dark patterns. The principal sources of dark patterns regulation, the UCPD, CPUT and the GDPR, have a wealth of case law and guidance in relation to unfair commercial practices and what is required for data protection respectively but these are largely not directly relevant to dark patterns or apply only by analogy.

There is some guidance, for example, as discussed above the EDPB released guidelines on dark patterns in social media platform interfaces.<sup>36</sup> The European Commission's guidance

29 *Ibid.* at Article 5(1)(a).

30 European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2. (October 20, 2020) 3.3 [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default\\_v2.0\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf).

31 *Ibid.* at Article 4.

32 *Ibid.* at Article 25.

33 European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, *supra* note 28 at 3.3.

34 Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*, 2019 O.J. C 112.

35 European Data Protection Board Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, *supra* note 6.

36 *Ibid.*

on the UCPD<sup>37</sup> also makes express reference to dark patterns and the CMA has published research (but not guidance) into Online Choice Architecture.<sup>38</sup> The European Commission's guidance notes the ability of businesses to use data to create persuasive practices that are personalized to the consumer and to continually adjust such practices to improve their effectiveness, observing that often such practices are employed without consumers' full knowledge.<sup>39</sup> It also raises concerns about A/B testing. However, this is all expressed in terms of generalities and concerns generally about "opaqueness,"<sup>40</sup> which in practice means that it is still hard to apply in a way that allows businesses to distinguish persuasive advertising or sales techniques from potentially manipulative commercial practices that are unfair under consumer law.

To illustrate the issues, take the example of an offer presented to a consumer attempting to cancel their subscription that provides 50 percent off the next 3 months if they choose to abandon cancellation. There are relatively strong arguments to support that this could be a dark pattern. It could be caught under the headings of Obstacles (for example as part of a roach motel) or Hindering (by prolonging the cancellation process by questioning the user's choice). There is, however, very little guidance or case law that provides a steer on whether this dark pattern (if it is such) is also contrary to the UCPD or CPUT or any other laws. There is nothing in the law that prescribes how cancellation of a subscription is to be achieved.

---

**“There is some guidance, for example, as discussed above the EDPB released guidelines on dark patterns in social media platform interfaces**

---

Certainly, preventing a consumer from exercising their legal rights to cancel a contract is highly problematic but what about presenting the consumer with an offer to keep the subscription at a discount? This is clearly a barrier to cancellation but is it a sufficient barrier such that it is tantamount to

preventing the consumer from exercising their rights of cancellation under the contract or their statutory right of withdrawal? Much will ultimately depend on how it is presented to the consumer and how easy it is in practice for that consumer to navigate around the offer and finally cancel their contract. The offer to keep the subscription might also be an unfair commercial practice or misleading under the UCPD or CPUT, but this is likely to hinge on how comparatively prominent the option to cancel is and how easy it would be for the consumer to exercise their cancellation rights. While some of the commentary in this area creates the impression that symmetry between the ease of sign up and cancellation is required in relation to subscriptions, there is at the time of writing no obvious basis for this in law.

Undoubtedly, case law and guidance will develop over time, but in the meantime, businesses are faced with difficult decisions in weighing up the risk of enforcement action, which may have the potential to cause serious reputational damage alongside potential fines and/or criminal law sanctions, against the advantages of designing their platforms so as to optimize sales and the communication of offers and deals to customers.

### ***B. Incoming Legislation Doesn't Quite Add Enough Color***

The DSA, which will apply to online platforms, will be the first piece of EU legislation that expressly bans dark patterns. However, the ban will only operate where existing laws on unfair commercial practices and the GDPR do not apply. It gives non-exhaustive examples of specific practices, such as subscription traps and giving more prominence to certain choices when asking a recipient of the service for a decision.<sup>41</sup> The DSA's explicit ban on dark patterns, on its face, should close a loop as it catches any use of dark patterns that is not in breach of the UCPD and the GDPR. However, two key challenges exist. The first is establishing whether the dark patterns in question are caught by one or other of these pieces of legislation. The second is applying the DSA's test of something that "deceives, manipulates or otherwise materially distorts a user's ability to make an informed decision."<sup>42</sup> This will be challenging without further guidance on how this is expected to be applied in practice. The DSA threatens

---

37 Guidance on the Unfair Commercial Practices Directive, *supra* note 20 at 4.2.7.

38 Competition & Markets Authority, *Online Choice Architecture: How digital design can harm competition and consumers*, (Discussion Paper CMA155, April 2022) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1066524/Online\\_choice\\_architecture\\_discussion\\_paper.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf) and Competition & Markets Authority, Evidence review of Online Choice Architecture and consumer and competition harm (Evidence Review CMA157, April 2022) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1069423/OCA\\_Evidence\\_Review\\_Paper\\_14.4.22.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069423/OCA_Evidence_Review_Paper_14.4.22.pdf).

39 Guidance on the Unfair Commercial Practices Directive, *supra* note 20 at 4.2.7.

40 *Ibid.* at 4.2.6.

41 Digital Services Act, *supra* note 2, at Article 25(3).

42 Digital Services Act, *supra* note 2, at Article 25(1).

large fines<sup>43</sup> which are surely intended to incentivize compliance, yet their deterrent effects may be hindered by a lack of clarity in respect of the DSA's jurisdiction over dark patterns.

That said, although we do not anticipate much actual enforcement under the DSA, it is significant that the EU considers dark patterns to be worthy of an express prohibition and this perhaps sets the tone for future enforcement and bans under the UCPD, CPUR or the GDPR given that the European Commission's stated view that these pieces of legislation are capable of capturing most dark patterns.<sup>44</sup>

The DSA is not the only place where we are seeing proposals to outlaw dark patterns in Europe. The EU's recently presented Data Act proposal<sup>45</sup> explicitly prohibits dark patterns. The most recent draft accepted by the Parliament applies to the manufacturers of connected products and providers of related services which are placed on the market in the EU and governs rights and obligations regarding the data generated by the use of the products and services. It sets out that data holders or third parties who receive the data of the user of the products or recipient of services from a data holder at the request of that user, are not to subvert or impair the autonomy of users to "coerce, deceive or manipulate" them in any way and therefore they should not use dark patterns in the design of the digital interface.<sup>46</sup> The Data Act proposal also states "[c]ommon and legitimate commercial practices that are in compliance with Union law should not in themselves be regarded as constituting dark patterns."<sup>47</sup>

Also proposed by the European Commission is the Artificial Intelligence (AI) Act<sup>48</sup> which incorporates what may be read as a limited prohibition on certain kinds of dark patterns. Under this draft legislation, "Prohibited Artificial Intelligence Practices" include AI systems that "deploy subliminal techniques"<sup>49</sup> or that exploit the vulnerabilities of a "specific group of persons due to their age, physical or mental disability"<sup>50</sup> with the intention to materially distort their behavior and in a manner that causes or

is likely to cause physical or psychological harm to that person or another.<sup>51</sup> This prohibition appears to have a relatively high threshold in order to be engaged as a result of the requirement that the distortion of behavior must be intended and "material," and the need for harm to be "physical or psychological harm." The UK has also looked at this issue as part of the UK consumer law refresh<sup>52</sup> which, at the time of writing, is still in progress and the draft Digital Markets Competition and Consumer Bill which is expected imminently. The UK government's approach appears to be that they will mirror the EU by commissioning further research and are contemplating an express ban – although this is not expected in the Bill.

In summary, dark patterns are high on the legislative and enforcement agenda in Europe. However, the law continues to be difficult to apply in the absence of practical guidance or a body of case law. It is also likely that deviations in the application of these laws will emerge across Europe as regulators attempt to utilize them to regulate dark patterns, which could result in certain forms of dark pattern being regarded as nothing more than a marketing technique in one jurisdiction but unlawful in another.

## 04 CONCLUSION

Recent activity such as the CPC sweep, the wave of letters from the Norwegian Consumer Council and the CMA's Online Choice Architecture Programme confirm that dark patterns are attracting considerable regulatory attention in Europe. No doubt enforcement will result and with this will come with publicized decisions that provide some clarity on

---

43 *Ibid.* at Article 53.

44 <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>.

45 Data Act Proposal, *supra* note 4 at Recital 34.

46 *Ibid.* at Article 6(2).

47 *Ibid.* at Recital 34.

48 Proposal for European Council Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts No. 2021/0106 (COD), 2021 COM(2021) 206 final (AI Act Proposal).

49 *Ibid.* at Article 5.

50 *Ibid.*

51 *Ibid.*

52 Department for Business, Energy and Industrial Strategy, Consultation outcome – Reforming competition and consumer policy: government response (CP 656, April 20, 2022) <https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy/outcome/reforming-competition-and-consumer-policy-government-response>.



where the legal lines are drawn. As new legislation outlawing dark patterns is introduced we can hope to see accompanying guidance or test cases that offer better insight into what this means for businesses who operate online interfaces and want to market effectively, but compliantly, to their customers. ■

---

“*The DSA is not the only place where we are seeing proposals to outlaw dark patterns in Europe*”

---

# CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit [competitionpolicyinternational.com](https://www.competitionpolicyinternational.com) today to see our available plans and join CPI's global community of antitrust experts.

