AT A GLANCE
Digital issues in focus

European Parliament

Regulating dark patterns in the EU: Towards digital fairness

Dark patterns are deceptive techniques used by online platforms to manipulate users' behaviour, often without their knowledge or consent. The EU regulatory framework against dark patterns is fragmented and lacks a unified legal definition. This can lead to legal uncertainty and inconsistent enforcement. Stakeholders and academics are calling for clearer definitions, stronger safeguards, and more effective enforcement of existing laws.

What are dark patterns?

Dark patterns or deceptive patterns can be described as 'tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something'. They are based on harmful online choice architecture. Their purpose is to influence a broad spectrum of consumer decisions, impeding the consumers' ability to make informed choices. They intentionally affect users' behaviour to manipulate them. Some dark patterns are designed to make the person feel compelled to purchase, either by the design of the website or by the 'opportunity' of the deal. Examples include fake urgency (for instance fake countdown timers) to pressure user action, disguised advertisement, and emotional manipulation to make users question their actions.

Absence of a single legal definition

There is no common definition of dark patterns in the EU legal framework. The Digital Services Act (DSA) describes them in its recital 67 as 'practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions'. According to the DSA, these practices are to be prohibited. The recent fitness check of EU consumer law on digital fairness defines dark patterns as 'unfair commercial practices deployed through the structure, design or functionalities of digital interfaces or system architecture that can influence consumers to make decisions they would not have taken otherwise'. The various definitions nevertheless have two key features in common: the manipulative or deceptive nature of the practice and the resulting negative or harmful outcome. As this description is quite broad, to be able to determine whether a particular practice should be classified as a dark pattern, there are numerous guidelines and practical recommendations to consider.

Complexity of the existing legislative framework

Dark patterns were introduced into the EU's legal framework by the Unfair Commercial Practices Directive (UCPD). However, the UCPD does not use the term 'dark patterns'. What it prohibits are 'misleading' and 'aggressive' commercial practices. The UCPD protects consumers against unfair business-to-consumer (B2C) commercial practices in advertising, sales and after-sales. To this 'first level' of protection, a series of subsequent legal acts were added, offering protection where the UCPD failed to offer adequate protection against new players and technological advances: the UCPD clearly forbids only a limited number of dark patterns that are mentioned in its Annex I and these prohibitions do not deal with digital interfaces.

The above-mentioned fitness check raised concerns about how Article 25 of the DSA interacts with other EU legal acts. While it prohibits online platforms from using dark patterns, it excludes practices covered by the UCPD and the General Data Protection Regulation (GDPR). This means that if a dark pattern of an online platform provider violates the GDPR, its legality will be assessed according to the requirements of the GDPR, not the DSA. This situation creates legal uncertainty. Although the GDPR does not address dark patterns explicitly, particular techniques to obtain consent from data users could be interpreted as such. This leaves space for interpretation that could minimise the impact of the DSA.

Similarly, the UCPD has such a broad scope, covering all B2C relations, that the space left for applying the DSA is limited. Consequently, the clear and general prohibition of dark patterns in the DSA may still lead to a reliance on the UCDP's case-by-case analysis. As a solution, the fitness check report proposed adding specific prohibitions of dark patterns to the UCPD. This could be done by expanding the UCPD's Annex I with explicit prohibitions addressing online interfaces.

Parliament's December 2023 resolution on addictive design of online service and consumer protection arrived at similar conclusions. It called on the Commission to close regulatory gaps relating to dark patterns, and strengthen transparency provisions, as the current rules were not sufficient to mitigate adverse effects. It argued that several dark patterns could already be addressed under the current list in Annex I of the UCPD. Nevertheless, it asked the Commission to assess the need to extend Annex I as a matter of urgency, to prohibit the most harmful practices. Parliament considered that development of ethical and fair digital products free of dark patterns should constitute reasonable professional diligence.

Other legal acts also address dark patterns. The Artificial Intelligence (AI) Act introduces new prohibitions on dark patterns, without mentioning the term specifically. The AI Act prohibits subliminal techniques, purposefully manipulative or deceptive techniques or use of AI systems that exploit vulnerabilities based on age, disability or a specific social or economic situation (Articles 5(1)(a) and (b)) that could cause significant harm. Unlike the DSA, the AI Act requires case-by-case interpretation of specific terms such as 'subliminal technique' and 'purposefully' manipulative or deceptive. However, exploitation of some vulnerabilities under the AI Act (e.g. emotion-recognition) is classified as high-risk AI, but not prohibited.

For its part, the Digital Markets Act (DMA) includes an anti-circumvention rule (Article 13) aimed at capturing dark patterns used by gatekeepers to influence consumer decisions unlawfully. The Data Act mentions the prohibition of the use of dark patterns in relation to third parties and data holders when they are designing their digital interfaces (Recital 38). These should not be designed in a way to make decisions unduly difficult for the users. Specific prohibition of dark patterns was introduced for financial services, with the 2023 amendment to the Consumer Rights Directive (CRD). The amendment (Article 16(e)) prohibits traders from applying dark patterns when they are concluding financial services contracts at a distance. This variety of provisions used in different legal acts intended to address dark patterns could create a lack of coherence in implementation. This was outlined in the above-mentioned fitness check report, which established a need for further action. Based on this evaluation, the Commission announced a public consultation in preparation for the upcoming Digital Fairness Act in 2025, to remedy the situation.

Academic views

Inge Graef warns of risk of inconsistencies, leading to under-enforcement owing to the fragmented EU regulatory framework for dark patterns. Martin Brenncke underlines the difficulty of effective regulation as dark patterns act in between legitimate persuasive techniques and illegal methods of coercion and manipulation. In addition, dark patterns take advantage of consumer behaviour bias, while EU consumer legislation assumes that consumers are rational economic actors. Mark Leiser and Cristiana Santos underline the importance of clear labelling of dark patterns in enforcement, and publicising such actions to discourage deception. In addition, they highlight the need to update the EU *acquis* constantly, to confront emerging prohibited designs and forms of manipulation (for instance hyper-nudging).

Stakeholder positions

During the public consultation for the digital fairness fitness check, stakeholders expressed concern about the current legal framework, citing ambiguity, complexity and ineffective enforcement. A majority of respondents advocated enhanced protection against dark patterns and similar deceptive practices, recommending clearer and stronger safeguards. They proposed, among other things, a comprehensive ban on dark patterns, clearer definitions of key concepts to reduce uncertainty, and the placing of a 'fairness by design' obligation on businesses.

The European Consumer Organisation, BEUC, recommended ensuring better enforcement against dark patterns and in particular, reviewing the UCPD and CRD. For the two directives, BEUC proposed to introduce an anti-circumvention clause, modelled on the example introduced by the DMA. A March 2024 BEUC report proposed regulatory solutions, based on a horizontal principle of fairness by design.

Digital industry stakeholders meanwhile insist that a distinction must be drawn between deceptive practices and legitimate online persuasive methods, so as not to jeopardise innovation. In a recent report, Eurocommerce argued that dark patterns are already sufficiently covered by existing legislation.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.