Page 816 - 833 **DOI:** *https://doi.org/10.63108/IJLMH.13244*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Regulating Dark Patterns on Digital Platforms: The European Union's Approach and Some Suggestions for Vietnam

NGUYEN QUOC ANH[*], DUONG BAO NGOC[**], AND DIEP BAO LONG[***]

ABSTRACT

Dark patterns, namely manipulative interface designs that influence users' decisions by exploiting cognitive biases, have emerged as a major challenge to consumer protection in the digital economy. While the European Union (EU) has developed a comprehensive regulatory framework for addressing dark patterns, Vietnamese law still lacks explicit legal provisions specifically governing these practices. Against this background, this paper examines the EU's legal approach to dark patterns and explores its implications for Vietnam. Employing doctrinal legal research together with legal analysis and comparative legal methods, the study analyses the concept, characteristics and harmful impacts of dark patterns, examines the interaction among the EU's principal regulatory instruments, and identifies the key features of the EU regulatory model. The findings indicate that the EU does not regulate dark patterns through a single legislative instrument. Instead, it has established an integrated regulatory framework that combines consumer protection law, data protection law and digital platform regulation to safeguard consumer autonomy. Nevertheless, challenges remain in distinguishing legitimate persuasive design from unlawful manipulative design and in ensuring coherent application across different regulatory instruments. Building on these findings, the paper proposes several recommendations for Vietnam in developing an appropriate legal approach to dark patterns. Academically, the study contributes to the growing scholarship on digital consumer protection by offering a systematic analysis of the EU regulatory model and demonstrating its value as a reference for future legal development in Vietnam.

Keywords: *Dark patterns, Autonomy, Consumer Protection, EU*

I. INTRODUCTION

The rapid expansion of the digital economy, e-commerce and online platforms has fundamentally transformed the way businesses engage with consumers. In the digital environment, competition is no longer confined to product quality, price or service; it has

[*] Author is a Student at Ha Noi Law University, Ha Noi, Viet Nam.
[**] Author is a Student at Ha Noi Law University, Ha Noi, Viet Nam.
[***] Author is a Student at Ha Noi Law University, Ha Noi, Viet Nam.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

increasingly shifted towards attracting, retaining and monetising users' attention. Against this background, the user interface no longer serves merely as a functional element facilitating the user experience; it has become a powerful tool capable of directly influencing consumer decision-making. By exploiting cognitive biases and psychological characteristics, businesses increasingly design online interfaces to steer, encourage or influence consumers' choices in ways that maximise commercial interests. These manipulative interface design techniques are commonly referred to as dark patterns.

Over the past decade, dark patterns have evolved from being viewed as a user-interface or user-experience design issue into a significant legal challenge across multiple areas of digital regulation. The 2024 online sweep of the International Consumer Protection and Enforcement Network (ICPEN), in which 27 consumer protection authorities from 26 countries took part, found that nearly 76% of the 642 subscription-based websites and applications reviewed employed at least one possible dark pattern, while nearly 67% used more than one.[1] Several high-profile cases further illustrate the seriousness of the issue. In 2019, for example, online accommodation booking platforms including Booking.com, Agoda and Hotels.com committed to changing their practices following enforcement action by the United Kingdom's Competition and Markets Authority (CMA) concerning misleading availability and popularity claims and other pressure-selling practices.[2] Likewise, the French data protection authority (CNIL) fined Facebook Ireland, Meta's European subsidiary, for designing a cookie interface that made it more difficult for users to refuse cookies than to accept them.[3]

In response to the growing prevalence of dark patterns, many jurisdictions and international organisations have gradually developed legal responses to these practices. Among them, the European Union (EU) is widely regarded as having adopted one of the most comprehensive and influential regulatory approaches. Rather than enacting a standalone statute specifically governing dark patterns, the EU has established a multi-layered legal framework through the combined application of the Unfair Commercial Practices Directive (UCPD), the General Data Protection Regulation (GDPR), the Digital Services Act (DSA) and other regulatory instruments and guidance. This integrated approach has significantly strengthened the regulation of

[1] Press Release, FED. TRADE COMM'N, *FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy* (July 10, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy (last visited Aug. 2, 2026).

[2] Press Release, COMPETITION & MARKETS AUTHORITY, *Hotel Booking Sites to Make Major Changes After CMA Probe* (Feb. 6, 2019), https://www.gov.uk/government/news/hotel-booking-sites-to-make-major-changes-after-cma-probe.

[3] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS [CNIL], Deliberation of the Restricted Committee No. SAN-2021-024 of 31 December 2021 Concerning Facebook Ireland Limited (Fr.).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

manipulative interface design in practice. Given its systematic structure and adaptability to the evolving digital environment, the EU regulatory model offers a valuable reference for jurisdictions seeking to enhance consumer protection in the digital economy, including Vietnam.

In Vietnam, the rapid expansion of e-commerce and digital platforms has been accompanied by the increasingly widespread use of practices exhibiting the characteristics of dark patterns in various forms. Although the existing legal framework contains a number of relevant provisions in consumer protection law, e-commerce regulation, advertising law and personal data protection law, it lacks specific legal provisions that explicitly address dark patterns as a distinct type of unlawful conduct. In this context, examining the legislative experience and enforcement practice of the European Union is of particular significance to the further development of Vietnam's legal framework for consumer protection in the digital environment.

Existing scholarship has examined dark patterns from various perspectives, including consumer protection, data protection and digital platform regulation. Further research is nevertheless needed to clarify how these regulatory instruments interact, to identify the strengths and limitations of the EU's multi-layered approach, and to assess the extent to which this experience can inform legal reform in jurisdictions with different institutional and regulatory conditions, particularly Vietnam. Accordingly, this study addresses two central questions: (i) what are the principal characteristics, strengths and limitations of the EU legal framework for regulating dark patterns? and (ii) which elements of this framework can appropriately be adapted to improve consumer protection under Vietnamese law? By addressing these questions, the study seeks to contribute to the comparative legal literature on dark patterns and to provide recommendations for the development of Vietnam's regulatory framework.

The study employs doctrinal legal research, analytical and synthetic methods, and comparative legal methods. The remainder of this paper is structured as follows. Section 2 provides an overview of dark patterns by examining their defining characteristics, common forms and harmful impacts on consumers. Building on this foundation, Section 3 examines the European Union's regulatory approach to dark patterns through its principal legal instruments and evaluates the strengths and remaining limitations of the current regulatory framework. Drawing on the EU experience, Section 4 proposes several recommendations for improving Vietnam's legal framework for protecting consumers against dark patterns on digital platforms. Finally, the conclusion summarises the principal findings and highlights the relevance of the EU experience for the future development of Vietnamese law.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

II. Overview of dark patterns on digital platforms

A. Concept and characteristics of dark patterns

The term "dark patterns" was introduced by the user-interface designer Harry Brignull in 2010 to refer to interface design techniques intentionally crafted to deceive, coerce or manipulate users into making decisions that are not in their best interest. The concept was developed in contrast to "design patterns", a well-established notion in interface design referring to reusable design solutions that address common usability problems and enhance the user experience.[4]

To date, there is no universally accepted definition of dark patterns. International organisations and regulatory authorities have approached the concept from different perspectives, depending on their regulatory objectives. At the European Union level, Recital 67 of the Digital Services Act (DSA) offers the first description of dark patterns in EU legislation, 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".[5] From a consumer protection perspective, the U.S. Federal Trade Commission (FTC) describes dark patterns as design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.[6] From a data protection perspective, the European Data Protection Board (EDPB) has described dark patterns as interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data.[7] Although no single definition has been universally accepted, the existing approaches suggest that dark patterns can generally be identified through three core characteristics. First, they employ interface design techniques or elements of digital choice architecture to influence users' behaviour. Second, they exploit users' cognitive biases and psychological vulnerabilities in order to alter their decision-making process. Third, they may result in adverse consequences for

---

[4] Harry Brignull, *Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff*, 90 Percent of Everything (July 8, 2010), https://deceptive.design/articles/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff; Colin M. Gray et al., *The Dark (Patterns) Side of UX Design*, in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, paper 534, at 3 (2018), https://doi.org/10.1145/3173574.3174108; *see also* Harry Brignull, *Deceptive Patterns: Get Started*, Deceptive Patterns (2023), https://deceptive.design/book/contents/get-started/ (last visited Aug. 10, 2026).

[5] 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 O.J. (L 277) 1, recital 67 [hereinafter DSA].

[6] Fed. Trade Comm'n, *Bringing Dark Patterns to Light* 2 (Staff Report, Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (last visited Aug. 10, 2026).

[7] European Data Protection Board, *Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them* 2 (version 1.0, Mar. 14, 2022).

users, including economic loss, diminished consumer autonomy and reduced control over personal data.

B. Forms and impacts of dark patterns

Common forms of dark patterns. To date, no universally accepted classification of dark patterns has emerged. Among the existing approaches, the taxonomy proposed by the Organisation for Economic Co-operation and Development (OECD) provides a useful framework for systematically classifying dark patterns.[8] Rather than merely cataloguing individual interface techniques, the OECD taxonomy groups dark patterns according to the behavioural manipulation mechanisms employed by businesses to undermine consumers' autonomy in decision-making.

Category	Name of dark pattern
Forced action	Forced registration; Forced disclosure / Privacy zuckering; Friend spam / Social pyramid / Address book leeching; Gamification
Interface interference	Hidden information; False hierarchy; Preselection; Misleading reference pricing; Trick questions; Disguised ads; Confirmshaming / Toying with emotion
Nagging	Nagging
Obstruction	Hard to cancel or opt out / Roach motel / Click fatigue / Ease; (Price) comparison prevention; Immortal accounts; Intermediate currency
Sneaking	Sneak into basket; Hidden costs / Drip pricing; Hidden subscription / Forced continuity; Bait and switch, including bait pricing
Social proof	Activity messages; Testimonials
Urgency	Low stock / High demand message; Countdown timer / Limited time message

Table 1: Categories and names of dark patterns. Source: OECD, Dark Commercial Patterns, OECD Digital Economy Papers No. 336, Annex B, at 53 (2022)

Although the OECD taxonomy distinguishes seven categories of dark patterns, these practices rarely occur in isolation. They are often combined within a single interface or deployed throughout the consumer journey, significantly increasing the likelihood that users will make decisions contrary to their preferences or best interests. More importantly, with the rapid development of big data, artificial intelligence (AI) and personalisation algorithms, dark patterns have evolved beyond conventional interface design techniques into data-driven and behaviour-based manipulation mechanisms. This evolution has further blurred the boundary

[8] OECD, *Dark Commercial Patterns* 53 (OECD Digital Economy Papers No. 336, Oct. 2022) (Annex B: Example of Consolidated Taxonomy of Dark Patterns).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

between legitimate marketing practices and manipulative interface design, while posing significant challenges to traditional legal and regulatory frameworks.

Harms of dark patterns. Dark patterns not only affect consumers but also have broader adverse effects on market competition and the healthy development of the digital economy. The major harm caused by dark patterns lies in the erosion of consumer autonomy in decision-making.[9] By exploiting cognitive biases and manipulating choice architecture, dark patterns do not necessarily deprive consumers of their ability to choose; rather, they interfere with the process through which choices are formed, leading consumers to make decisions that do not reflect their actual preferences or interests. Dark patterns may consequently give rise to three major forms of consumer harm. First, economic harm occurs when consumers incur additional costs or enter into or remain in transactions that they did not intend. Second, privacy and data protection harms may arise where interface design facilitates the collection of personal data by default or makes refusing or withdrawing consent significantly more difficult than giving it. Third, psychological and time-related harms may result from prolonged or repeated interactions with manipulative interfaces, contributing to decision fatigue, stress and increased time spent on digital platforms, particularly where platform business models depend on capturing and retaining user attention.

Beyond individual consumer harm, dark patterns may also distort competition in digital markets. Rather than competing on product quality, innovation or price, businesses may gain a competitive advantage through manipulative interface design. This may create incentives for competitors to adopt similar practices in order to remain competitive, contributing to a "race to the bottom" in which standards of transparency and responsible interface design progressively decline.[10] Over time, the widespread use of dark patterns may further undermine consumer trust in digital platforms, increase transaction costs and hinder the sustainable development of e-commerce.

Taken together, these concerns demonstrate that dark patterns are no longer merely a matter of interface design or user experience but constitute a broader legal challenge in the digital economy. Their diverse forms, their capacity to exploit cognitive biases, and their adverse effects on both consumers and market competition expose the limitations of relying solely on traditional rules concerning unfair commercial practices and information disclosure. Effective regulation therefore requires a more comprehensive approach that not only addresses harmful

[9] OECD, *supra* note 8, at 23–24.
[10] M.R. Leiser, *'Dark Patterns': The Case for Regulatory Pluralism* (SSRN Working Paper, 2020), https://doi.org/10.2139/ssrn.3625637; *see also* OECD, *supra* note 8, at 13, 26–27.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

practices after they occur but also incorporates preventive safeguards at the interface-design stage, thereby preserving consumers' ability to make free and informed decisions.

III. The European Union's legal framework for regulating dark patterns

A. Components of the European Union's legal framework

General Data Protection Regulation (GDPR).[11] One of the interests infringed by dark patterns is the protection of personal data, as users are guided or manipulated into consenting to the collection, use or sharing of their personal data in a manner that does not reflect their genuine will. Within the European Union, the General Data Protection Regulation serves as the central legal instrument governing the processing of personal data, thereby providing an important legal basis for regulating privacy dark patterns. The GDPR was adopted as Regulation (EU) 2016/679; it entered into force on 24 May 2016 and has applied since 25 May 2018, replacing Directive 95/46/EC (the Data Protection Directive) with the aim of establishing a harmonised legal framework for the protection of personal data throughout the European Union. Compared with Directive 95/46/EC, the GDPR strengthens the rights of data subjects while expanding the responsibilities of data controllers and data processors in the digital environment.

The GDPR establishes a comprehensive system of rights to ensure that data subjects maintain control over their personal data throughout the data processing lifecycle. In the context of dark patterns, these rights not only serve as mechanisms for protecting the lawful rights and interests of data subjects but also provide a legal basis for assessing the lawfulness of interface designs that may distort or impede users' decision-making processes.

First, the GDPR recognises the right to be informed and the right of access, enabling data subjects to know what personal data are being processed, the purposes of processing, the retention period, and other information relating to the processing of their personal data. These rights are particularly significant in addressing interface interference practices, such as hidden information, disguised ads and trick questions, as such interface designs often conceal or misrepresent information, thereby preventing users from making decisions on the basis of complete and accurate information.

In addition, the GDPR guarantees the right to withdraw consent at any time where the processing of personal data is based on the data subject's consent. This right plays an important

[11] 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 O.J. (L 119) 1, arts. 5(2), 7(3), 12–18, 20, 21, 25, 99.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

role in limiting dark patterns such as confirmshaming and false hierarchy, which are designed to steer users into consenting to the processing of their personal data or to create psychological barriers when they seek to change their decision.

Furthermore, the GDPR recognises the right to erasure, the right to restriction of processing, the right to data portability and the right to object. These rights are particularly significant in addressing obstruction practices, such as "hard to cancel" and the "roach motel", which obstruct or prolong the exercise of users' rights after their personal data have been collected. By granting data subjects these rights, the GDPR not only ensures control over personal data at the point of collection but also enables data subjects to maintain such control throughout the entire data processing lifecycle.

In addition to recognising a range of rights of data subjects, the GDPR imposes key obligations on data controllers to ensure that these rights are effectively exercised in practice; in certain circumstances, data processors are likewise required to comply with corresponding obligations. First, these actors are responsible for ensuring transparency in data processing by providing users with information that is adequate, clear and easily accessible. In addition, the GDPR requires the application of the principle of data protection by design and by default, whereby interfaces must be designed in a manner that protects personal data and facilitates the exercise of users' rights. Furthermore, through the principle of accountability, the GDPR requires data controllers to demonstrate compliance with data protection requirements throughout the processing.

These provisions provide an important legal basis for enforcement authorities in the European Union to prevent dark patterns that infringe the right to the protection of personal data.

Unfair Commercial Practices Directive (UCPD).[12] While the GDPR focuses on protecting personal data against privacy dark patterns, the UCPD approaches the issue from the perspective of protecting consumers' transactional decisions and economic interests against commercial dark patterns. Accordingly, the UCPD is an important legal instrument governing unfair commercial practices between businesses and consumers. It was adopted in 2005 and subsequently amended by Directive (EU) 2019/2161, known as the Omnibus Directive. The UCPD has progressively adapted to the development of e-commerce and the digital environment, thereby providing a legal basis for addressing various interface manipulation practices that may distort consumers' transactional decisions.

[12] 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 (Unfair Commercial Practices Directive), 2005 O.J. (L 149) 22 [hereinafter UCPD].

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The UCPD does not directly regulate dark patterns but instead establishes general criteria for assessing the lawfulness of commercial practices. Under the general clause in Article 5(2) of the UCPD, a commercial practice is unfair if it is contrary to the requirements of professional diligence and materially distorts or is likely to materially distort the economic behaviour of the average consumer. From this perspective, the UCPD focuses on preventing commercial practices that may affect consumers' transactional decisions.

First, Articles 6 and 7 of the UCPD require traders to ensure the transparency of information throughout the transaction process with consumers. Accordingly, businesses must not provide misleading information, conceal material information, or present information in a manner that is likely to mislead consumers about the nature, characteristics or conditions of a transaction. On this basis, various dark patterns that may mislead consumers, such as concealing material information, disguising advertising content or creating a false hierarchy of choices, may be assessed as unfair commercial practices.

Second, Articles 8 and 9 protect consumers' freedom of choice and transactional decision-making by prohibiting practices that involve harassment, coercion or undue influence in the decision-making process. Even in the absence of traditional forms of coercion, interface designs intended to influence or distort consumers' transactional decisions, or to make it difficult for consumers to reject or terminate a transaction, may also be assessed as unfair commercial practices.

Third, through the amendments introduced by the Omnibus Directive, the UCPD was adapted to commercial practices in the digital environment, in particular through provisions concerning the authenticity of online reviews and the transparency of the main parameters determining the ranking of search results; the same Directive amended the Consumer Rights Directive to require traders to inform consumers when a price has been personalised on the basis of automated decision-making.[13] These amendments demonstrate that EU consumer law has progressively adapted to the development of e-commerce and the digital economy, thereby enhancing its capacity to protect consumers from increasingly diverse dark patterns in practice.

The Digital Services Act (DSA). Alongside the rapid development of the digital age, there has been a growing proliferation of manipulative interface design strategies that affect consumer

[13] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 Amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as Regards the Better Enforcement and Modernisation of Union Consumer Protection Rules, 2019 O.J. (L 328) 7, arts. 3(4), 4(4) [hereinafter Omnibus Directive] (inserting UCPD arts. 7(4a), 7(6) and Consumer Rights Directive 2011/83/EU art. 6(1)(ea)).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

decision-making.[14] Against this background, the existing legal instruments of the European Union have increasingly revealed certain regulatory gaps, while public and regulatory awareness of deceptive design techniques used to manipulate user behaviour has continued to grow.[15] In response to these developments, the adoption of the Digital Services Act in 2022 marked a significant new development in EU legislation.

The Digital Services Act establishes binding legal requirements for the integrity of digital interface design. It treats manipulative interface practices as violations of the principles of transparency, fairness and user protection in the digital environment, in the following ways.

First, the EU legal framework recognised the concept of manipulative interface practices for the first time in Recital 67 of the DSA. The recital describes such practices as those that materially distort or impair users' ability to make autonomous and informed choices or decisions on online platforms. The recital also provides examples of manipulative interface designs and draws a boundary by emphasising that not every form of influence on user behaviour constitutes a manipulative interface practice. This reflects the legislator's effort to strike a balance between protecting users and safeguarding businesses' freedom to conduct their commercial activities. From a legislative perspective, however, the recital cannot be regarded as a legal definition in the strict sense, as the description is not included in the DSA's definitions provision. It is nevertheless the first time that EU law has formally described the nature of manipulative interface practices, thereby providing an important basis for the interpretation and application of Article 25 DSA.

Second, the DSA clarifies the obligations of online platform providers regarding user interfaces. Article 25(1) prohibits three forms of conduct that interfere with users' autonomy through the design, organisation or operation of interfaces, namely: (i) deceiving users; (ii) manipulating users; and (iii) otherwise materially distorting or impairing users' ability to make free and informed decisions. This provision reflects a preventive approach by requiring compliance from the design and development stage of an interface, rather than intervening only after harm has occurred, as was the case with traditional mechanisms established under earlier legal frameworks. At the same time, Article 25(3) empowers the European Commission to issue guidelines on how the prohibition applies to specific practices, notably the three groups of practices it lists. These practices are not exhaustive, which gives the competent authorities

[14] Kadir Deligöz, *Consumer Manipulation With Artificial Intelligence: Dark Patterns and Hidden Techniques*, in CONSUMER, MARKETING, AI: DARK SIDES AND ETHICS 201 (Kürşad Özkaynar & Şevin Abbasoğlu eds., Özgür Publications 2025).

[15] Xin Ye, *Dark Patterns and Addictive Designs*, 5(3) WEIZENBAUM J. DIGIT. SOC'Y 3–5 (2025), https://doi.org/10.34669/wi.wjds/5.3.2.

sufficient flexibility to respond to the rapid development and changing forms of manipulative interface practices. In practice, the DSA's rules on dark patterns have already been invoked in enforcement. In its investigation of Meta, for example, the European Commission preliminarily found that Facebook and Instagram appeared to use dark patterns in their "Notice and Action" mechanisms and failed to provide a user-friendly and easily accessible procedure for users to report illegal content.[16]

Third, Article 25(2) of the DSA establishes a relationship between the DSA, the UCPD and the GDPR: the prohibition in Article 25(1) does not apply to practices covered by the UCPD or the GDPR. This provision, however, raises concerns about the practical effectiveness of Article 25 in prohibiting manipulative interface practices. Cristiana Santos et al. argue that almost all forms of manipulative interface practices identified to date could fall within the scope of either the GDPR or the UCPD.[17] Article 25 may therefore provide only a limited level of additional protection beyond that already offered by existing legal instruments. Moreover, this mechanism may lead to fragmentation and overlap within the legal framework governing manipulative interface practices, as the same practice may fall under several legal instruments, requiring a determination of which instrument takes priority. This not only makes it more difficult to identify the applicable legal basis and the enforcement authority, but may also create gaps in consumer protection.

Fourth, the DSA establishes a strict system of sanctions. Providers may be fined up to 6% of their annual worldwide turnover for failing to comply with their obligations under the DSA, and up to 1% of their annual income or worldwide turnover for supplying incorrect, incomplete or misleading information or failing to submit to an inspection; they may also be subject to periodic penalty payments of up to 5% of their average daily worldwide turnover or income to compel compliance.[18] These penalties exceed the minimum set by earlier rules such as the UCPD, which, as amended by the Omnibus Directive, requires the maximum fine for widespread infringements subject to coordinated enforcement to be at least 4% of the trader's

[16] Press Release, EUROPEAN COMMISSION, *Commission Preliminarily Finds TikTok and Meta in Breach of Their Transparency Obligations Under the Digital Services Act* (IP/25/2503, Oct. 24, 2025), https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503 (last visited Aug. 1, 2026).

[17] Cristiana Santos et al., *Which Online Platforms and Dark Patterns Should Be Regulated Under Article 25 of the DSA?* 3–4 (SSRN Working Paper, 2024), https://doi.org/10.2139/ssrn.4899559; *see also* Fabrizio Esposito, Cecilia Isola, Cristiana Santos & Martim Farinha, *Back to the Future-Proof: Four Reforms for the Better Regulation of Dark Patterns Under the Unfair Commercial Practices Directive and Article 25 of the Digital Services Act*, EUR. J. RISK REGUL. 1, 14 (2026), https://doi.org/10.1017/err.2026.10088.

[18] DSA, *supra* note 5, arts. 52(3)–(4), 74(1)–(2), 76(1).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

annual turnover in the Member States concerned.[19] This places greater pressure on digital platforms to prioritise compliance with their legal obligations.

Other relevant legal instruments. In addition to the key legal instruments discussed above, the EU legal framework includes several other instruments containing provisions that address manipulative interface practices. These include the following.

The Digital Markets Act (DMA).[20] The DMA was adopted to regulate large digital platforms that provide core platform services and hold significant market power, such as Meta and Apple's App Store. Article 13 establishes an anti-circumvention rule to prevent such gatekeepers from using manipulative interface practices to undermine users' choices: under Article 13(6), a gatekeeper must not make the exercise of the rights or choices laid down in the Act unduly difficult, including by offering choices in a non-neutral manner or by subverting users' autonomy, decision-making or free choice via the structure, design, function or manner of operation of a user interface. The protected rights and choices include the rule in Article 5(2) that a gatekeeper may not repeat a refused request for consent for the same purpose more than once within a period of one year, which aims to prevent nagging, and the obligation under Article 6(3) to allow users to easily uninstall pre-installed applications, which aims to prevent obstruction. These provisions help limit the power of large digital platforms and strengthen the protection of users' autonomy.

The Data Act.[21] Although the Data Act is not a consumer protection instrument, it plays a complementary role in this area. Like the DSA, the Data Act refers to dark patterns in its recitals, in Recital 38. There is, however, a difference between the two approaches. The Data Act describes dark patterns as design techniques that push or deceive consumers into decisions that have negative consequences for them, whereas the impairment of users' ability to make autonomous and informed choices is the central element of the DSA's description. In addition, the Data Act establishes prohibitions applicable both to data holders (Article 4(4)) and to third parties receiving data (Article 6(2)(a)). Under these provisions, both are prohibited from making the exercise of users' choices or rights unduly difficult, including by offering choices in a non-neutral manner or through the design or operation of a user digital interface.

---

[19] UCPD, *supra* note 12, art. 13(3) (as substituted by Omnibus Directive, *supra* note 13, art. 3(6)).

[20] 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 O.J. (L 265) 1, arts. 5(2), 6(3), 13(6).

[21] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), O.J. L, 2023/2854, recital 38, arts. 4(4), 6(2)(a).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The Artificial Intelligence Act (AI Act).[22] The development of AI has enabled more personalised and sophisticated forms of manipulative interface practices, as algorithms can analyse user behaviour and predict psychological vulnerabilities to optimise manipulative techniques. The AI Act prohibits AI systems that deploy subliminal techniques or purposefully manipulative or deceptive techniques (Article 5(1)(a)), and AI systems that exploit people's vulnerabilities due to age, disability or a specific social or economic situation (Article 5(1)(b)), where such practices materially distort behaviour in a manner that causes or is reasonably likely to cause significant harm. Compared with the UCPD, the AI Act has a broader scope because it is not limited to activities carried out for commercial, advertising or business purposes. The Act nevertheless has certain limitations. These practices are prohibited only when they are carried out through an AI system, leaving other technological means outside its scope. In addition, the categories of vulnerable persons listed in the Act may not cover all groups that could be vulnerable to such practices.

Overall, the EU legal framework on manipulative interface practices is diverse, covering different types of harm and different digital contexts. This diversity, however, creates a significant challenge by making the legal framework more complex and potentially less consistent in practice. The concern has also been identified in the European Commission's Digital Fairness Fitness Check, which assessed the effectiveness of the existing framework.[23] Against this background, in its 2026 Work Programme the European Commission announced, under the priority "Protecting our democracy, upholding our values", a legislative initiative for the fourth quarter of 2026, the Digital Fairness Act (DFA).[24] The initiative aims to address the current limitations of the EU legal framework and strengthen consumer protection.

B. Evaluation of the European Union's legal framework

Appropriate aspects of the EU legal framework for Vietnam. Based on the analysis above, the EU legal framework governing manipulative interface practices has several significant advantages and progressive features. In the current context, these rules are not only valuable as a legislative reference but also contain several elements that are relevant to Vietnam's needs and conditions for developing and improving its legal framework, as follows.

---

[22] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), O.J. L, 2024/1689, art. 5(1)(a)–(b).

[23] EUROPEAN COMMISSION, *Questions and Answers on the Digital Fairness Fitness Check* (QANDA/24/4909, Oct. 3, 2024), https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_4909 (last visited Aug. 4, 2026).

[24] EUROPEAN COMMISSION, *Commission Work Programme 2026*, COM (2025) 870 final, annex I, item 30 (Oct. 21, 2025), https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2026_en (last visited Aug. 4, 2026).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

First, the EU legal framework adopts a multi-layered approach to regulating manipulative interface practices comprehensively. This approach rests on the fact that manipulative interface practices can occur in various contexts, ranging from e-commerce, social media and mobile applications to virtual assistants and IoT devices. At the same time, such practices may affect different interests, including consumer autonomy, personal data protection and privacy. Odise Xhelita and Apostolos Manthos argue that, by their nature, manipulative interface practices lie at the intersection of consumer protection law, digital regulation and personal data protection law.[25] A single legal instrument therefore cannot address all forms and effects of these practices. A multi-layered approach allows competent authorities to use different legal instruments to address different aspects of the same manipulative practice. This approach is relevant to Vietnam because the existing Vietnamese legal system already has a structure and legislative direction that can support it. Vietnam has enacted several legal instruments regulating different aspects of the digital environment, such as the Law on Protection of Consumers' Rights 2023, the Law on Personal Data Protection 2025, the Law on Electronic Transactions 2023, and Decree No. 147/2024/ND-CP on the management, provision and use of Internet services and online information.[26] Although these instruments do not directly regulate manipulative interface practices, they have established a basic legal foundation for Vietnam to draw on the EU's experience and gradually improve the existing legal framework in response to the development of the digital environment.

Second, EU law has established specific and direct rules governing manipulative interface design, including provisions on the concept of manipulative interface practices, prohibitions, specific obligations concerning interface design on digital platforms, and sanctions. The EU has also developed detailed guidance to help identify and classify different forms of manipulative interface practices. This is important because it provides competent authorities with a clear legal basis to identify, assess and address such practices, while also promoting consistency in enforcement. At the same time, it provides digital platforms with clearer standards that allow them to comply with their legal obligations from the product design stage. The EU's approach has been described as regulating for consumer autonomy,[27] and it is strongly preventive. Rather than focusing only on the consequences of manipulative practices, it shifts attention towards the

[25] Odise Xhelita & Apostolos Manthos, *Dark Patterns on the Internet Under the EU Consumer Law*, in STRATEGIC INNOVATIVE MARKETING AND TOURISM 863 (Springer 2025), https://doi.org/10.1007/978-3-031-81962-9_93.
[26] Luật Bảo vệ quyền lợi người tiêu dùng [Law on Protection of Consumers' Rights], No. 19/2023/QH15 (June 20, 2023) (Viet.); Luật Bảo vệ dữ liệu cá nhân [Law on Personal Data Protection], No. 91/2025/QH15 (June 26, 2025) (Viet.); Luật Giao dịch điện tử [Law on Electronic Transactions], No. 20/2023/QH15 (June 22, 2023) (Viet.); Decree No. 147/2024/ND-CP on the Management, Provision and Use of Internet Services and Online Information (Nov. 9, 2024) (Viet.).
[27] Martin Brenncke, *Regulating Dark Patterns*, 14 NOTRE DAME J. INT'L & COMP. L. 39 (2024).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

structure and operation of digital interfaces that may distort or significantly impair users' decision-making. This represents a relatively new approach to regulation, addressing technological risks at an early stage and thereby contributing to more effective protection of consumer autonomy on digital platforms.

In contrast, Vietnamese law still shows significant gaps in protecting digital consumers compared with the EU legal framework. One notable difference is the lack of clear legal provisions and guidance addressing the technical dimensions of digital design. Vietnamese law currently relies mainly on general provisions. For example, the Law on Protection of Consumers' Rights 2023 prohibits operators of digital platforms from restricting consumers' right to choose by prioritising certain products, goods or services without publicly disclosing the selection criteria,[28] while the Law on Personal Data Protection 2025 requires that a data subject's consent not be accompanied by a condition compelling consent to purposes other than those agreed.[29] It can therefore be seen that Vietnam is still at an early stage in developing a legal framework for consumer protection in the digital environment. Existing rules mainly focus on preventing the consequences of conduct or ensuring the outcome of a transaction, rather than establishing specific obligations concerning the design and operation of digital interfaces that may influence user behaviour. This creates significant gaps in the legal framework and may allow businesses to take advantage of these gaps to implement manipulative techniques.

Against this background, it is necessary and appropriate for Vietnam to study the EU legal framework systematically and selectively when improving its consumer protection policies. This relevance is further supported by the close alignment between the EU's legislative approach and Vietnam's current direction for developing the digital environment. Resolution No. 57-NQ/TW of 22 December 2024 of the Politburo on breakthroughs in the development of science, technology, innovation and national digital transformation states that people and businesses are at the centre of, and the main actors in, this development, and calls for building a safe and healthy digital society.[30] Drawing on the EU's experience would therefore not only help Vietnam better protect consumer autonomy on digital platforms but also ensure consistency with the legislative direction and development strategies established in Vietnam's current policy documents.

[28] Law on Protection of Consumers' Rights, No. 19/2023/QH15, *supra* note 26, art. 10(3)(b).
[29] Law on Personal Data Protection, No. 91/2025/QH15, *supra* note 26, art. 9(4)(b).
[30] Nghị quyết số 57-NQ/TW của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia [Resolution No. 57-NQ/TW of the Politburo on Breakthroughs in the Development of Science, Technology, Innovation and National Digital Transformation] pts. I(2), III(5) (Dec. 22, 2024) (Viet.).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Inappropriate aspects of the EU legal framework for Vietnam. Although the European Union's legal framework is regarded as one of the pioneering frameworks for regulating dark patterns and serves as an important reference for Vietnam, not all of the EU's rules and approaches are suitable for adoption. In particular, the framework still presents several limitations that should be taken into account when drawing on its legislative experience.

First, the legal framework has not established sufficiently clear criteria to distinguish between lawful persuasive interface design and prohibited dark patterns. Although EU law has begun to recognise the concept and various forms of dark patterns, the existing rules have yet to establish a clear framework for identifying such practices in practice. In particular, the existing instruments have not established a unified set of legal criteria for drawing the boundary between lawful persuasive design and unlawful manipulative design. For example, whether highlighting a button through its colour, size or position on the interface to attract users' attention is merely a measure to optimise the user experience or amounts to a dark pattern remains unclear. Even Harry Brignull, who coined the term "dark patterns", has noted that distinguishing between persuasive and manipulative design is highly challenging in practice, because it depends on the context, purpose and actual impact of the interface on users' behaviour.[31]

Enforcement practice in the European Union also reflects these difficulties. In the case concerning the cancellation process for Amazon Prime, which was examined by the European Commission and the Consumer Protection Cooperation (CPC) Network, the reported cancellation practices involved complicated navigation menus, skewed wording, confusing choices and repeated nudging, yet the matter was resolved through commitments following a dialogue rather than by a formal finding that the interface constituted a dark pattern. The authorities primarily required the company to modify the cancellation process to make it simpler and more transparent.[32] This demonstrates that the identification of dark patterns still depends significantly on the assessment of enforcement authorities in each specific case, reflecting a gap in objective legal criteria for distinguishing between lawful persuasive design and unlawful manipulative practices.

Second, some legal terms and the mechanisms for coordinating the UCPD, the GDPR and the DSA remain complex and insufficiently clear. On the one hand, many legal terms in the DSA, such as "deception", "manipulation" and "autonomy", are not defined in the legislation; on the other hand, the DSA does not have as well-established a foundation of guidance as the UCPD,

[31] HARRY BRIGNULL, DECEPTIVE PATTERNS: EXPOSING THE TRICKS TECH COMPANIES USE TO CONTROL YOU ch. 12 (Testimonium 2023), https://deceptive.design/book/contents/chapter-12.

[32] Press Release, EUROPEAN COMMISSION, *Consumer Protection: Amazon Prime Changes Its Cancellation Practices to Comply With EU Consumer Rules* (IP/22/4186, July 1, 2022).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

which has accumulated over the past 20 years, nor does it contain sufficient references or connections to the conceptual framework and criteria developed under the UCPD. Consequently, enforcement authorities still have to refer to the UCPD's doctrines, guidance and case law to interpret Article 25 of the DSA. This may make it difficult for the DSA to achieve the effectiveness expected of sector-specific legislation designed to address complex technical issues.[33] In addition, the coordination between the DSA, the GDPR and the UCPD in regulating dark patterns in the European Union remains a major bottleneck, as analysed in Section 3.1. Fabrizio Esposito and his co-authors liken the resulting system to "spaghetti code", with rules that are intertwined and overlapping but lack logical coherence.[34] This undermines the effectiveness of the EU's system for protecting users against dark patterns.

IV. SUGGESTIONS FOR VIETNAM

From the legislative experience of the EU, Vietnam can draw several important orientations in the process of perfecting its legal framework on dark patterns.

First, Vietnam should review and introduce clear, specific and direct legal provisions governing the design of digital platform interfaces, including definitions, obligations and clear prohibitions on the use of manipulative interface practices within the national legal framework. This could be achieved by making use of Vietnam's existing legal framework, for instance by amending and supplementing the Law on Protection of Consumers' Rights 2023 or the Law on Personal Data Protection 2025, or by adopting a specific Government decree on digital platforms. The development of these provisions should, however, ensure consistency with the terms and concepts already used in existing legislation. It is also necessary to define their scope of application clearly and to establish flexible mechanisms for coordination between different legal instruments in order to avoid overlap or gaps in enforcement. These measures would help address existing legal gaps and strengthen consumer protection on digital platforms.

Second, in addition to legal documents, Vietnam should consider issuing detailed guidance to establish technical standards and a classification system for manipulative interface practices, as well as potentially developing a national code of ethics for digital interface design. In particular, technical standards should seek to establish a clear boundary between persuasive design and manipulative design. These measures would help reduce inconsistent interpretation and application of the law, improve the transparency and feasibility of legal provisions, and enable

[33] Esposito et al., *supra* note 17, at 3, 8.
[34] Esposito et al., *supra* note 17, at 4.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

businesses to comply proactively while allowing competent authorities to monitor and address manipulative interface practices more effectively.

Third, when establishing sanctions for manipulative interface practices, Vietnam should consider extending turnover-based fines to the field of consumer protection, without necessarily adopting the same level of fines as the EU. Compared with fixed fines, turnover-based sanctions are more proportionate to the size of a business and can provide a stronger deterrent for digital platforms, while also providing more effective protection for consumers' autonomy and freedom of choice. In addition, sufficiently strong sanctions would encourage businesses to comply with legal requirements from the design and development stage of digital interfaces, thereby contributing to a more transparent, fair and consumer-centred digital business environment.

V. CONCLUSION

This paper demonstrates that dark patterns have become a significant challenge to consumer protection in the digital environment, while traditional legal rules are increasingly insufficient to address manipulative interface design. Through a comparative analysis, the paper shows that the European Union has established a relatively comprehensive regulatory framework by combining the GDPR, the UCPD, the DSA and related instruments with active enforcement and interpretative guidance. By contrast, although Vietnamese law contains provisions on consumer protection, e-commerce and personal data protection, it still lacks a coherent approach specifically governing dark patterns. Building on this analysis, the paper suggests that Vietnam should introduce clear legal provisions defining and prohibiting dark patterns while coordinating the legal instruments that govern them, develop more detailed guidance and technical standards for digital platform design, and consider turnover-based sanctions. By providing a systematic examination of the EU approach and its relevance to Vietnam, this study contributes to the ongoing discussion on modernising consumer protection law in the digital economy.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]