

## **Protecting User Autonomy in the Digital Age: Assessing the European Union’s Consumer Protection Framework Amid the Rise of Dark Patterns**

By Brandon King<sup>1</sup>

*Dark patterns are manipulative design techniques built into digital interfaces, such as countdown timers on e-commerce sites or online services that are easy to sign up for but difficult to cancel, which exploit cognitive biases and undermine user autonomy. As digital commerce expands across the European Union (EU), these practices have become an increasing threat to the continent’s digital consumers. This paper argues that while the EU’s current consumer protection framework, including the Digital Services Act (DSA), General Data Protection Regulation (GDPR), Unfair Commercial Practices Directive (UCPD), and related laws provide a solid foundation, they are fragmented and inconsistent in addressing the emerging challenges posed by dark patterns. Drawing on the philosophical concepts of substantive, procedural, and relational autonomy, this paper assesses the extent to which EU legislation preserves consumer decision-making power in digital markets. This paper draws on empirical studies to demonstrate that dark patterns are both widespread and effective in manipulating online behavior, particularly among vulnerable populations. To address these challenges, this paper advocates for the creation of a Dark Pattern Protection Act (DPPA) that consolidates the current overlapping legislation, introduces a harmonized definition of what constitutes dark patterns, and establishes both a centralized enforcement through the European Commission for large multinational entities and also member-level coordinators to enforce the act against smaller violators. This proposed framework would strengthen consumer protection and ensure that user autonomy remains a central tenet of digital regulation within the EU.*

---

<sup>1</sup> Brandeis University, Class of 2026.



The rise of the digital age has revolutionized the nature of commerce and upended traditional commercial practices, introducing new complexities for businesses, consumers, and regulators around the world.<sup>2</sup> One of the most consequential technological developments of the digital age has been the rise of dark patterns: manipulative design practices and techniques embedded within the user interface (UI) of digital commerce platforms.<sup>3</sup> Dark patterns have fundamentally changed the nature of consumer interactions and behaviors while online, often to the consumer's detriment.<sup>4</sup> The need to protect consumers from the dangers of dark patterns is pressing in a time where 93% of the European Union's (EU) population aged 16-74 regularly accesses the internet, and 72% of this population engages in e-commerce. These consumers fuel an e-commerce industry on the continent that generates €958 billion in annual revenue, with a projected growth rate of eight percent per year.<sup>5</sup> Given the substantial population of users impacted by dark patterns, safeguarding user autonomy from this growing threat is critical.<sup>6</sup> Addressing the challenge of safeguarding user autonomy from dark patterns requires an evaluation of the EU's current legal and regulatory landscape governing consumer protection. This paper argues that while the EU's consumer protection framework is strong, it is not sufficiently comprehensive to ensure the strongest level of safeguarding consumer autonomy from dark patterns, due to

---

<sup>2</sup> Gillian K. Hadfield, *Privatizing Commercial Law: Lessons from the Middle and the Digital Ages* (Mar. 1 2000).

<sup>3</sup> Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Leg. Anal. 43 (2021).

<sup>4</sup> Car Palona, *Regulating Dark Patterns in the EU: Towards Digital Fairness* | Think Tank | European Parliament, (Jan. 13, 2025)

<sup>5</sup> Luca Cassetti & Christel Delberghe, *European E-Commerce Report 2024*, Cent. Mark. Insights Amst. Univ. Appl. Sci. Ecommerce Eur. EuroCommerce 91 (2024).

<sup>6</sup> M. Brennecke, *A Theory of Exploitation for Consumer Law: Online Choice Architectures, Dark Patterns, and Autonomy Violations*, 47 J. Consum. Policy 127 (2024).



confusion arising from overlapping legislation and directives. It proposes a remedy to this problem in the form of consolidating the overlapping laws, definitions, directives, and policies, and a refinement of the existing regulatory structure into a new Dark Pattern Protection Act.

### **I. Defining User Autonomy**

The philosophical concept of autonomy has been the subject of significant academic debate going back centuries to the times of Ancient Greece, where it was studied by some of the most influential philosophers, including Socrates, Plato, and Aristotle, who discussed it at great length.<sup>7</sup> Aristotle offered a perspective on autonomy that applies to the current issue, defining it as an individual's ability to deliberate and make choices (prohairesis).<sup>8</sup> Modern philosophers have expanded upon this concept of autonomy to address the challenges faced by online consumers in the digital age.<sup>9</sup> Substantive Autonomy, a concept developed by Joseph Raz, is the notion that "autonomy is based upon relevant options to choose from as well as the capacity to make the choice".<sup>10</sup> Procedural Autonomy, a concept developed by Gerald Dworkin, is the notion of the "capacity of an individual to critically reflect on, endorse, or revise their own motivations, preferences, and decisions, and to act in accordance with that reflection".<sup>11</sup> Relational Autonomy, a concept developed by Jennifer Nedelsky and Catriona Mackenzie, is the idea that autonomy "emerges from social relationships, power dynamics,

---

<sup>7</sup> *Introduction: Socrates and the Precept "Know Yourself", in Socrates and Self-Knowledge 1 (Christopher Moore ed., 2015)*

<sup>8</sup> Richard Kraut, *Aristotle's Ethics*, in *The Stanford Encyclopedia of Philosophy* (Edward N. Zalta & Uri Nodelman eds., Fall 2022 ed. 2022), <https://plato.stanford.edu/archives/fall2022/entries/aristotle-ethics/>.

<sup>9</sup> Joseph Raz, *The Morality of Freedom* (1986).

<sup>10</sup> *Id.*

<sup>11</sup> Lawrence Haworth, *Dworkin on Autonomy*, 102 *ETHICS* 129 (1991).



and structural conditions.”<sup>12</sup> The application of these philosophical definitions of autonomy by the EU is critical for the regulation of dark patterns. To safeguard consumer autonomy from dark patterns, legislation and its subsequent enforcement must preserve an individual’s substantive, procedural, and relational autonomy; however, this must be balanced against the legitimate business interests of sellers within digital markets.

## II. Definition of Dark Patterns

Currently the EU lacks a harmonized definition within its legal framework of what constitutes a dark pattern practice.<sup>13</sup> The EU, through various pieces of legislation, has defined and barred specific commercial practices, creating a quasi-definition of practices which could be construed as dark patterns.<sup>14</sup> However, the lack of consistency within EU law weakens the overall consumer protection regime and undermines the goal of safeguarding user autonomy from such manipulative practices.<sup>15</sup>

The Digital Services Act (DSA), implemented in 2022, defines dark pattern practices in 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.”<sup>16</sup> This definition, while clear, does not align precisely with the definition provided by the Fitness Check of EU Consumer Law on Digital Fairness (DFC). The DFC, while not a piece of legislation, is an

---

<sup>12</sup> Natalie Stoljar, *Feminist Perspectives on Autonomy*, in *The Stanford Encyclopedia of Philosophy* (Edward N. Zalta & Uri Nodelman eds., Summer 2024 ed. 2024),

<sup>13</sup> Palona, *supra* note 4.

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance) of 2022, 277 OJ L.



important policy document that defines dark patterns as “unfair commercial practices deployed through the structure, design or functionalities of digital interface for system architecture that can influence consumers to take decisions they would not have taken otherwise.”<sup>17</sup> These definitions have slight but material differences such as the DSA’s focus on users’ ability to make ‘autonomous and informed decisions’ while focusing only on online platforms.<sup>18</sup> The DFC focuses on the manipulation aspect of dark patterns and their impact on consumers making choices that could be contrary to their interests and often their intent.<sup>19</sup> The DFC also analyzes a wider range of digital settings by stating ‘digital marketplaces’ rather than the DSA’s application to ‘online platforms.’<sup>20</sup>

While the EU provides different definitions of dark patterns, academic literature has taken into account additional factors that directly impact user autonomy. One definition created by Dr. Lugari of Yale University and Dr. Strahilevitz of the University of Chicago in their article *Shining a Light on Dark Patterns*, defines dark patterns as:

“User interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. They typically exploit cognitive biases and prompt online consumers to purchase goods and services that they do not want or to reveal personal information they would prefer not to disclose.”<sup>21</sup>

This definition adds a component to the impact of dark patterns not expressed directly in the text of EU law: the psychological forces and cognitive biases of consumers that

---

<sup>17</sup> COMMISSION STAFF WORKING DOCUMENT FITNESS CHECK of EU Consumer Law on Digital Fairness, (2024),

<sup>18</sup> Palona, *supra* note 4.

<sup>19</sup> COMMISSION STAFF WORKING DOCUMENT FITNESS CHECK of EU consumer law on digital fairness, *supra* note 17.

<sup>20</sup> Palona, *supra* note 4.

<sup>21</sup> Luguri and Strahilevitz, *supra* note 3.



dark patterns seek to exploit.<sup>22</sup> Incorporation of these considerations into EU law is essential for safeguarding user autonomy from dark patterns.

### III. Prevalence of Dark Patterns

One of the first academic studies to examine the prevalence of dark patterns was conducted in 2019 by a research team from Princeton University and the University of Chicago.<sup>23</sup> In this study, computer scientists analyzed 53,000 product display pages (PDPs) across 11,000 popular e-commerce websites and found that 11% of these websites employed dark pattern practices.<sup>24</sup> In addition to identifying the overall presence of dark pattern practices, the study identified a correlation between a website's popularity and its likelihood of employing dark pattern practices, concluding that the more popular a website was, the more likely it was to employ dark patterns. Beyond websites, e-commerce platforms on digital interfaces, such as applications built on the Android and IOS operating systems, often have a higher prevalence of dark patterns.<sup>25</sup> A 2020 study by researchers at the University of Zurich found that 95% of free applications available for download in the United States Google Play store contained dark patterns.<sup>26</sup> These studies highlight that dark patterns are highly prevalent on digital commerce platforms regardless of the interface, emphasizing the urgent need for specific legislation to protect users' autonomy while online.

---

<sup>22</sup> *Id.*

<sup>23</sup> Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 Proc ACM Hum-Comput Interact 81:1 (2019).

<sup>24</sup> *Id.*

<sup>25</sup> Linda Di Geronimo et al., *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems 1 (2020), <https://dl.acm.org/doi/10.1145/3313831.3376600>.

<sup>26</sup> *Id.*



#### IV. Efficacy of Dark Patterns

The prevalence of dark patterns is widespread within the domain of digital commerce, and their effectiveness in manipulating consumers to act against their own interests is equally significant.<sup>27</sup> In a study conducted by Dr. Lugari and Dr. Strahilevitz, they found that when no dark patterns were used, only 11.3% of users selected a certain setting on a website, which rose to 25.8% for the experimental group exposed to mild dark pattern conditions, and 41.9% for the experimental group exposed to aggressive dark pattern conditions.<sup>28</sup> These results corroborate additional recent academic studies, such as one conducted by researchers at Cambridge University, which found that dark pattern practices significantly increased the probability of users participating in a course of action beneficial to the seller and contrary to the user's interests and desired course of action.<sup>29</sup> Additionally, the study discovered that individuals based on characteristics such as minors, minimal levels of education, and lacked moderate to high levels of wealth were at greater risk of the effects of dark patterns while online.<sup>30</sup> These studies highlight the prevalence and efficacy of dark patterns within the digital landscape, where online sellers and platforms utilize these practices to their advantage, often at the expense of consumer autonomy.

#### V. The EU's Current Consumer Protection Regime

Through decades of creating legislation and enforcement regimes, the EU has a strong consumer protection regime.<sup>31</sup> Within the current framework, several pieces of

---

<sup>27</sup> Luguri and Strahilevitz, *supra* note 3.

<sup>28</sup> *Id.*

<sup>29</sup> Amit Zac et al., *Dark Patterns and Consumer Vulnerability*, *Behav. Public Policy* 1 (2025).

<sup>30</sup> *Id.*

<sup>31</sup> *Consumer Protection Measures | Fact Sheets on the European Union | European Parliament*, (Apr. 30, 2024), <https://www.europarl.europa.eu/factsheets/en/sheet/47/consumer-protection-measures>.



legislation have a role in protecting consumers from dark patterns, which are mentioned below.<sup>32</sup>

### A. The Digital Services Act (DSA)

The DSA, as implemented in 2022, is intended to protect consumers from illegal content, increase the transparency and accountability of online platforms, ensure fairness and respect for fundamental rights while online, and provide legal certainty within this area of law across the EU.<sup>33</sup> As mentioned previously, the DSA directly defines and prohibits certain dark patterns within their legislation.<sup>34</sup> Enforcement of the DSA is delegated to ‘digital service coordinators’ at the member state level for platforms targeting a country’s respective citizens.<sup>35</sup> For platforms with over 45 million monthly active users in the EU (VLOPs and VLOSEs), the European Commission serves as the principal regulator.<sup>36</sup>

---

<sup>32</sup> *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1; 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 (General Data Protection Regulation) [2016] OJ L119/1; Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) [2005] OJ L149/22; Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights (Consumer Rights Directive) [2011] OJ L304/64; 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 (Data Act) [2023] OJ L2023/2854; 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 (Digital Markets Act) [2022] OJ L265/1.*

<sup>33</sup> *The EU’s Digital Services Act*, (Oct. 27, 2022), [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/euro-pe-fit-digital-age/digital-services-act\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/euro-pe-fit-digital-age/digital-services-act_en).

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*



## B. The Data Act

The Data Act, implemented in 2024, regulates access to non-personal data generated by connected devices and services.<sup>37</sup> Article 3(3) of the Act grants users “easy access to the data they generate and the ability to give or withdraw consent in an understandable, non-misleading manner.”<sup>38</sup> Article 4(6) of the Act states that “data holders must present terms in a transparent and comprehensible format.”<sup>39</sup> Enforcement of the Data Act is delegated to regulators at the Member State level, with the European Commission monitoring Member State enforcement measures.<sup>40</sup>

## C. General Data Protection Regulation (GDPR)

The EU’s GDPR, implemented in 2018, protects individuals’ personal data and ensures “transparent, fair, and lawful data processing practices.”<sup>41</sup> Although dark patterns are not explicitly mentioned, the regulation addresses manipulative design practices that may constitute dark patterns.<sup>42</sup> Article 4(11) and Article 7 require that consent be “freely given, specific, informed, and unambiguous,” while Article 7(3) mandates that withdrawing consent must be “as easy as giving it.”<sup>43</sup> The act further states in Articles 12 to 14 that data subjects should receive “clear and accessible information about data processing activities.”<sup>44</sup> The European Data Protection Board (EDPB), which oversees continental oversight of GDPR enforcement, published Guidelines 3/2022, condemning

---

<sup>37</sup> *Data Act Explained | Shaping Europe’s Digital Future*, <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained> (last visited Apr. 18, 2025).

<sup>38</sup> *ibid*

<sup>39</sup> *ibid*

<sup>40</sup> *Data Act explained | Shaping Europe’s digital future*, *supra* note 37.

<sup>41</sup> *General Data Protection Regulation (GDPR) Compliance Guidelines*, GDPR.eu, <https://gdpr.eu/> (last visited Apr. 20, 2025).

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*



interface-based dark patterns such as “overloading, skipping, stirring, and hindering.”<sup>45</sup> Enforcement of GDPR is delegated to Data Protection Authorities (DPAs) at the Member State level, and the EDPB manages cross-border enforcement to ensure “consistent application” across the EU.<sup>46</sup>

#### **D. The Unfair Commercial Practices Directive (UCPD)**

The UCPD, implemented in 2007, provides a strong layer of consumer protection through Article 5(2), which establishes that commercial practices are prohibited if they “materially distorts or [are] likely to materially distort the economic behaviour of the average consumer,” Article 5(3) lays out even stronger protections for “vulnerable consumers.”<sup>47</sup> Additionally, the UCPD also includes an annex of 31 blacklisted commercial practices always deemed to be unfair.<sup>48</sup> Enforcement of the UCPD is delegated to national regulators within respective Member States.<sup>49</sup>

#### **E. Consumer Rights Directive (CRD)**

The CRD, implemented in 2014, provides additional protections to consumers through mandating sellers provide “clear and comprehensive details before a sale” (Articles 5-6), providing consumers with a right to withdraw from a contract for any reason within 14 days (Articles 9-16), and mandating “specific consent” from consumers regarding the purchase of

---

<sup>45</sup> *Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them* | European Data Protection Board, [https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media\\_en](https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en) (last visited Apr. 20, 2025).

<sup>46</sup> General Data Protection Regulation (GDPR) Compliance Guidelines, *supra* note 41.

<sup>47</sup> *Unfair Commercial Practices Directive - European Commission*, [https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-and-price-indication/unfair-commercial-practices-directive\\_en](https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-and-price-indication/unfair-commercial-practices-directive_en) (last visited Apr. 20, 2025).

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*



add-ons and subscriptions.<sup>50</sup> Enforcement of the directive is delegated to national regulatory agencies.<sup>51</sup>

### **F. Digital Markets Act (DMA)**

The final piece of relevant legislation is the DMA, implemented in 2023, which exclusively targets digital “gatekeepers.”<sup>52</sup> The act bans “deceptive, unclear, or manipulative UI to obtain consent (Article 13),” it requires gatekeepers to make “unsubscribing as easy as subscribing” (Article 6(11)), and mandates gatekeepers present “clear and fair choice screens for core services” (Article 6(12)).<sup>53</sup> Enforcement of this Act is done at the continental level through the European Commission.<sup>54</sup>

## **VI. Proposed Recommendations to Safeguard User Autonomy**

In order to safeguard user autonomy in light of dark patterns, the EU should adopt targeted legislation that incorporates provisions from the existing consumer protection regime, while harmonizing and modernizing these provisions to meet the unique challenge posed by dark patterns. The intent should be to protect consumers’ economic interests as well as their substantive, relational, and procedural autonomy. The current consumer protection regime is an assortment of overlapping laws that address a broad spectrum of issues both

---

<sup>50</sup> *Consumer Rights Directive - European Commission*, (Feb. 27, 2018), [https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/consumer-rights-directive\\_en](https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/consumer-rights-directive_en).

<sup>51</sup> *ibid.*

<sup>52</sup> *The Digital Markets Act: Ensuring Fair and Open Digital Markets - European Commission*, [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/euro-pe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/euro-pe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en) (last visited Apr. 20, 2025).

<sup>53</sup> *Id.*

<sup>54</sup> *ibid.*



online and offline.<sup>55</sup> While this strategy may have sufficed in the past, the emergent complexities of dark patterns require a more precise response.

Rather than starting from scratch, the EU should incorporate and build upon the aforementioned consumer protection provisions related to dark patterns to develop a comprehensive “Dark Pattern Protection Act” (DPPA). This approach would enable a smooth transition among the relevant stakeholders who are already familiar with the current regime. Additionally, this harmonization preserves the judicial history and decades of established case law, a benefit that would be lost if the EU started from a blank slate. The structure of the “DPPA” should be modeled on the UCPD with the implementation of a “catch-all” clause, similar to Articles 5(2-3), which evaluates a practice’s impact on users’ substantive, relational, and procedural autonomy while balancing legitimate business interests of sellers within digital markets. The “DPPA” should also include an annex containing blacklisted practices that automatically constitute prohibited dark patterns.

Implementing the DPPA in the manner described in this paper would materially strengthen the substantive, relational, and procedural autonomy of EU consumers within the online domain. With respect to substantive autonomy, the DPPA enhances the supply-side conditions under which consumer choice is exercised by expanding optionality in digital markets through the prohibition of manipulative interface designs, including complex or asymmetric user interfaces that render unsubscribing, declining consent, or cancelling services intentionally difficult, thus enabling consumer decisions to reflect the respective consumer’s preferences.<sup>56</sup> The DPPA would also enhance relational autonomy by recalibrating the

---

<sup>55</sup> Dan Jerker B. Svantesson, *Enter the Quagmire – the Complicated Relationship between Data Protection Law and Consumer Protection Law*, 34 *Comput. Law Secur. Rev.* 25 (2018).

<sup>56</sup> Joseph Raz, *The Morality of Freedom* (1986).



asymmetrical power dynamics that currently exist within online transactions between sellers and consumers, as digital vendors presently enjoy a material informational and structural advantage derived from their access to consumer data, behavioral analytics, and the deployment of dark pattern practices that often operate beyond the consumer awareness.<sup>57</sup> By restricting such practices, the DPPA limits a sellers' ability to covertly steer consumer behavior and restores a more balanced relational framework helping to preserve consumer agency.<sup>58</sup> Lastly, the DPPA advances procedural autonomy through its annex of blacklisted practices and the broad catch-all provision, which in tandem work to preclude manipulative sales techniques that exploit the cognitive biases of consumers, including artificial countdown timers that induce urgency or false scarcity claims that suggest limited product availability.<sup>59</sup> Taken as a whole, the DPPA does not merely regulate deceptive design practices but fundamentally restructures the conditions of online choice, transforming the nature of consumer autonomy within the digital market places that exist within the EU.

Additionally, the DPPA should be drafted and interpreted by national and European level courts as the primary authority in all cases involving allegations of dark pattern practices by sellers or platforms. This separation would allow for the decoupling of overlapping current consumer protection provisions and enable more targeted enforcement. From an enforcement perspective, the Act should be modeled on the DSA with 'DPPA enforcement coordinators' at the Member State level enforcing the "DPPA" in the Member State's national interest, while making the European

---

<sup>57</sup> Lawrence Haworth, *Dworkin on Autonomy*, 102 *Ethics* 129 (1991).

<sup>58</sup> *Id.*

<sup>59</sup> Natalie Stoljar, *Feminist Perspectives on Autonomy*, in *The Stanford Encyclopedia of Philosophy* (Edward N. Zalta & Uri Nodelman eds., Summer 2024 ed. 2024), <https://plato.stanford.edu/archives/sum2024/entries/feminism-autonomy/>.



Commission the principal regulator for the “DPPA” in relation to VLOPs and VLOSEs. This approach represents the most effective path forward by introducing a new, harmonized act that not only consolidates existing consumer protection provisions related to dark patterns but also allows legislators to incorporate additional measures to address emerging technologies, such as generative AI, within this new framework.

The DPPA would address prevailing concerns of the current consumer protection regime's ability to protect user autonomy in the age of dark patterns. These include the concerns of academics such as Dr. Graef of Tilburg University, who warned in an EU policy paper of “inconsistencies, leading to under-enforcement owing to the fragmented EU regulatory framework for dark patterns.”<sup>60</sup> It alleviates the concerns of Dr. Brenneke of Aston Law School, who warned of the “difficulty of effective regulation as dark patterns act in between legitimate persuasive techniques and illegal methods of coercion,” as the catch-all provision of the DPPA, balancing consumer autonomy, will serve as the legal test constituting what practices should be considered dark patterns.<sup>61</sup>

## VII. Conclusion

In an increasingly digital world, safeguarding user autonomy from dark patterns is a regulatory necessity. While the EU's existing consumer protection regime provides a strong foundation, it requires an updated harmonization to meet the evolving challenges of dark patterns. A targeted, comprehensive “DPPA” would preserve legal continuity, enhance enforcement, and integrate emerging technologies into the law. Thus, ensuring consumers' substantive, relational, and procedural autonomy from dark patterns, as digital commerce continues to expand across the EU.

---

<sup>60</sup> Palona, *supra* note 4.

<sup>61</sup> *ibid*

