Tackling Dark Patterns through the EU legal framework

Benjamin Lim

University of Edinburgh

s2599925@ed.ac.uk

December 15, 2024

1. Introduction

Brignull first coined the term Dark Patterns in 2010, defining it as "a user interface that has been carefully crafted to trick users into doing things" [1]. Dark Patterns are incorporated into products with the aim of misleading the user into performing an action that is favorable to the business, such as additional spending or sharing of data which the user did not originally intend for.

Since its formal recognition and definition, it has been observed on numerous websites, with over 400 examples documented in a "hall of shame" [2]. An OECD report has also cited multiple studies where 60% to 90% of websites globally were observed to utilize Dark Patterns [3]. Due to its prevalence and impact on consumer welfare, there have been attempts to regulate its use. In this essay, I will be attempting to loosely categorize Dark Patterns into five categories, those that hide information, those that go one step further to sow confusion, those that go even further to present false information, and those that go the furthest by obstructing users. Finally, I will look at those which exploit human psychology. For each category, I will be highlighting the successes of EU's regulatory efforts in addressing dark patterns through regulation, cases, as well as enforcement notices. I will then use empirical data to explain why these efforts are only moderately successful, and end with a final note on recent developments in this area of law.

2. Overview of the EU Legal Framework

There are two key EU instruments tackling the issue of Dark Patterns, the Unfair Commercial Practices Directive (UCPD) [4], as well as the General Data Protection Regulation (GDPR) [5]. The UCPD aims to protect consumer rights through regulating unfair business prac-

1 Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (1st, 2023), pp. 7

2 H Brignull and others, 'Deceptive Patterns - Hall of Shame' (25 April 2023) <https://www.deceptive.design/hall-of-shame> accessed 2 November 2024

3 OECD, 'Dark commercial patterns' (2022) 336 OECD Digital Economy Papers <https://doi.org/10.1787/44f5e846-en>, Annex C

4 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

6 Dir 2005/29/EC (n 4), art. 1

tices such as Dark Patterns [6]. At a high level, the UCPD targets misleading as well as aggressive commercial practices [7]. As we will explore later, most Dark Patterns aim to mislead consumers, hence the UCPD is usually the most appropriate tool in the legislative toolbox.

The GDPR is a close second place in effectiveness at addressing Dark Patterns. The GDPR's primary aim is to protect personal data [8]. To do so, it mandates "informed consent" as a condition for lawful processing [9] and requires that personal data is processed in a "transparent manner" [10], which would not be possible if pertinent information about data processing was hidden from consumers through deliberate design decisions such utilization of Dark Patterns.

Apart from the UCPD and the GDPR, Dark Patterns would under certain circumstances also fall under the ambit of the Consumer Rights Directive (CRD) [11], the Misleading and Comparative Advertising Directive (MCAD) [12], the Directive on Privacy and Electronic Communications (ePrivacy Directive) [13], as well as the Electronic Commerce Directive (e-Commerce Directive) [14]. In the following sections, I will first explore the successes that each of these instruments have in addressing certain types of Dark Patterns, before concluding with an analysis of how these instruments interplay, and the potential gaps that exists in the legal framework.

3. Addressing Dark Patterns which hide information

"Hidden Costs" and "Hidden Subscriptions" are examples of Dark Patterns which hide information from consumers [15]. Businesses choose to hide information about additional costs or subscriptions at the initial stages, revealing them to the customer only at the final page before payment or in the following month's invoice. "Visual Interference" and "Sneaking" are also examples[16] of Dark Patterns which hides information visually through font size, colour, placement or by presenting the information only after a delay. Such practices contravene Article 7(2) of the UCPD which states that "hid[ing] or provid[ing] in an unclear" manner any information that would influence a consumer to make a decision "he would not have taken otherwise" is a misleading omission [17]. In proceedings against Canal Digital, information about an additional six-monthly card service fee was omitted from

7 Dir 2005/29/EC (n 4), sect. 1 and 2

8 reg 2016/679 (n 5), art. 1

9 reg 2016/679 (n 5), recital. 32

10 reg 2016/679 (n 5), art. 5(1)(a)

11 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Counci [2011] OJ L304/64

12 Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising [2006] OJ L376/21

13 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)) [2002] OJ L201/1

14 Directive 2000/31/EC Of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1

15 H Brignull and others, 'Deceptive Patterns' (25 April 2023) <https://www.deceptive.design/types> accessed 2 November 2024

16 Brignull and others, 'Deceptive Patterns' (n 15)

17 Dir 2005/29/EC (n 4), art. 7(2)

the banner ads and displayed in an inconspicuous manner in their television advertisements [18]. The CJEU affirmed that such a practice would constitute an omission if the consumer was misled into a decision but left the referring court to make that assessment [19]. Thus, it can be concluded that Article 7(2) of the UCPD is effective at tackling Dark patterns which hide information, with the caveat that the claimant is able to prove that the omission induced him to enter the contract.

Article 6(1)(o) of the CRD requires businesses engaging in distance contracts to provide information about contract duration and conditions for termination to the consumer [20]. In 2019, Xbox membership subscription and auto renewal details were hidden from users [21]. After an investigation conducted by the Competition and Markets Authority (CMA), Microsoft voluntarily improved the user interface to disclose required details [22]. The CRD is therefore also effective at ensuring that information about subscriptions and renewals are not hidden using the "Hidden Subscriptions" Dark Patterns.

Lastly, article 5(1)(a) of the GDPR requires that personal data is processed in a "transparent manner" [23], hence businesses are forbidden from using "Visual Interference" when seeking consent from users. In 2023, The Italian Data Protection Agency (DPA) ruled against Edis-com S.p.A as the latter placed the option to opt-out at the bottom of the page, outside the pop-up and in a smaller font size [24]. This ruling was significant as Dark Patterns was explicitly mentioned in the decision.

4. Addressing Dark Patterns which create confusion

Apart from hiding information, another strategy used by Dark Patterns is to create confusion. With "Disguised Ads", advertisements are deliberately styled in a similar manner to the page content so as to confuse consumers into inadvertently clicking them [25]. "Trick wording" makes use of complex language to confuse customers as to the true meaning of the statement [26]. Article 7 of the UCPD prohibits misleading omissions [27]. To provide greater legal certainty, the UCPD includes a list of practices considered as misleading or aggressive in Annex I [28]. Item 11 of Annex I mandates that in instances where the "trader has paid for the promotion", it must be made "clearly identifiable by the consumer" [29]. Hence, using Dark Patterns to disguise advertising is considered a misleading omission under the UCPD. In Peek & Cloppenburg, although the nexus of the case revolved around whether payment included both monetary and in kind, the court nonetheless confirmed the im-

18 Case C-611/14 *Anklagemyndigheden v Canal Digital Danmark A/S* ECLI:EU:C:2016:800, para. 17-20

19 *Anklagemyndigheden v Canal Digital* (n 18), para. 64

20 Dir 2011/83/EU (n 11), art. 6(1)(o)

21 Competition and Markets Authority, *CMA secures changes to Xbox subscription practices* (2022) <https://www.gov.uk/government/news/cma-secures-changes-to-xbox-subscription-practices> accessed 8 November 2024

22 Competition and Markets Authority, *CMA secures changes to Xbox subscription practices* (n 21)

23 reg 2016/679 (n 5), art. 5(1)(a)

24 Cristiana Santos and Arianna Rossi, 'The emergence of dark patterns as a legal concept in case law' (31 July 2023) <https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept> accessed 8 November 2024

25 Brignull and others, 'Deceptive Patterns' (n 15)

26 Brignull and others, 'Deceptive Patterns' (n 15)

27 Dir 2005/29/EC (n 4), art. 7

28 Dir 2005/29/EC (n 4), annex. I

29 Dir 2005/29/EC (n 4), annex. I, Item 11

portance of the UCPD in "protect[ing] the consumer against covert advertising" [30].

Under Article 4(a) of the MCAD, comparative advertising is permitted if it is *inter alia* not misleading [31]. Hence, using trick wording to mislead consumers into favouring a business over its competitors contravenes the directive. In Carrefour v ITM Alimentaire, Carrefour was alleged to have compared the prices of its products in its larger hypermarts to its competitor's smaller supermarkets [32]. Larger stores generally benefit from economies of scale and hence, the use of trick wording in performing the comparison was seen by the courts as misleading [33].

5. Addressing Dark Patterns which present false information

Some Dark patterns go a step further than just creating confusion, they present false information to the consumer. Businesses use "Fake scarcity", "Fake urgency" and "Fake social proof" to deceive customers into purchasing products by convincing them that the product is low on stock, that the supposed discounted price is only valid for a short time, or that other customers have positive reviews of the product [34]. Article 6(1)(b) of the UCPD requires that business do not falsify availability of a product, Article 6(1)(d) tackles the issue of fake discounted price validity and Article 6(2) addresses the issue of using falsified reviews in marketing [35]. CMA filed an enforcement order against Viagogo for the practice of reducing the number of available tickets on the website in real time, when there were no such sales occurring at that point in time [36]. Although there was a subsequent judgement for contempt of court, the issue of falsifying real time sales was no longer brought up [37], hence it can be surmised that Viagogo ceased the practice after receiving the enforcement order.

Apart from Article 6(1)(d) of the UCPD, Article 6(c) of the e-Commerce Directive also addresses the issue of false discounts by requiring that "promotional offers" be displayed "clearly and unambiguously" [38]. The European Consumer Protection Cooperation (CPC) took action against Expedia for falsely presenting a standard price as a discounted price, misleading consumers to believe that they enjoyed "genuine saving" [39]. Subsequently, Expedia "implemented an audit process on discounts" to remediate the issue [40].

Finally, on the topic of "Fake social proof",

30 Case C-371/20 *Peek & Cloppenburg KG v Peek & Cloppenburg KG* ECLI:EU:C:2021:674, para. 45

31 Dir 2006/114/EC (n 12), art. 4(a)

32 Case C-562/15 *Carrefour Hypermarchés SAS v ITM Alimentaire International SASU* ECLI:EU:C:2017:95, para. 9

33 *Carrefour v ITM Alimentaire* (n 32), para. 40

34 Brignull and others, 'Deceptive Patterns' (n 15)

35 Dir 2005/29/EC (n 4), art. 6(1)(b), art. 6(1)(d) and art. 6(2)

36 High Court of Justice, *Competition and Markets Authority and Viagogo AG - Enforcement Order* (2018) <https://assets.publishing.service.gov.uk/media/5bffe2afe5274a0fae2c5397/CMA_v_Viagogo_Order_27.11.pdf> accessed 10 November 2024, para. 22c

37 *Viagogo AG v Competition and Markets Authority* [2019] EWHC 1706

38 Dir 2000/31/EU (n 14), art. 6

39 European Commission, *Expedia enforcement action* (2020) <https://commission.europa.eu/system/files/2020-12/factsheet-expedia_enforcement_action_1.pdf> accessed 10 November 2024

40 European Commission, *Expedia enforcement action* (n 39)

41 Competition and Markets Authority, *Transparency of heating oil price comparison websites* (2011) <https://www.gov.uk/cma-cases/transparency-of-heating-oil-price-comparison-websites> accessed 10 November 2024

WCF Limited was found to have displayed unsubstantiated customer testimonials on their website, Fuelfighter.co.uk [41] in contravention on Article 6(2) of the UCPD [42]. After an investigation by CMA, the business and its owners undertook to stop the practice of misleading consumers [43]. Having observed three cases where businesses improved their user interfaces after having been served enforcement notices for contravening the UCPD, it can be argued that the UCPD is a very effective instrument against businesses that exploit Dark Patterns to present false information.

6. Addressing Dark Patterns which obstruct customers

Certain Dark Patterns forgo the smoke and mirrors and simply obstruct customers from trying to perform an intended action. "Forced Action" bundles multiple actions and forces the customer to make an all or nothing decision [44]. "Hard to Cancel" makes it extremely tedious for customers to cancel as compared to the sign-up process [45]. Finally, "Obstruction" is as described and requires no further explanation [46]. Recital 43 of the GDPR requires "separate consent" for "different personal data processing operations" [47]. This ensures that the data subject is freely consenting to every single operation and not reluctantly consenting to some operations that were bundled with others. In the European Data Protection Board (EDPB)'s decision regarding TikTok, TikTok was found to have bundled the creation of an account together with the decision to make the account public [48]. Thus, users who wanted to create a TikTok account were forced into a public account at the time of creation, the implications of which, the Ireland DPA described as "particularly severe and wide-ranging". It is also poignant to note that the German DPA considered this as an example of a Dark Pattern [49]. A compliance order was issued [50], and TikTok is currently appealing the decision [51]. Regardless of the outcome of the appeal, this case serves as a cautionary tale to the public, who would be deterred from utilizing dark patterns that are proscribed under the GDPR.

The ePrivacy directive requires that prior consent is sought from the subscriber when engaging in direct marketing [52]. The ePrivacy directive uses the same definition of consent as the GDPR [53]. Hence, we can derive that withdrawal of consent under ePrivacy directive must be "as easy as" providing consent [54]. The rationale is that if the data subject intends to withdraw consent but is unable to jump through all the hoops required, then the data subject did not willingly

42 Dir 2005/29/EC (n 4), art. 6(2)

43 Competition and Markets Authority, *Transparency of heating oil price comparison websites* (n 41)

44 Brignull and others, 'Deceptive Patterns' (n 15)

45 Brignull and others, 'Deceptive Patterns' (n 15)

46 Brignull and others, 'Deceptive Patterns' (n 15)

47 reg 2016/679 (n 5), recital. 43

48 European Data Protection Board, *Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)* (2023) <https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf>, para. 31

49 European Data Protection Board (n 48), para. 45

50 European Data Protection Board (n 48), para. 287

51 Case T-1030/23 *Tiktok Technology v European Data Protection Board* (ECJ)

52 Dir 2002/58/EU (n 13), para. 42

53 Dir 2002/58/EU (n 13), para. 17

54 Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (2017) <https://ec.europa.eu/newsroom/article29/items/623051>, pp. 17

consent to continued processing, and thus the consent obtained is not freely given. The "Hard to Cancel" Dark Pattern thus violates the ePrivacy directive [55]. In the Monetary Penalty Notice issued by the Information Commissioner's Office (ICO) against We Buy Any Car (WBAC) Limited, it was remarked that WBAC used an "unconventional definition" of all communication that excluded marketing messages [56] that made it hard for customers to opt out of receiving such messages. As a result, WBAC was fined under the ePrivacy directive for the usage of the "Hard to Cancel" Dark Patterns [57].

According to Article 4(11) of the GDPR, consent from the data subject has to be "informed" and "freely given" [58]. To fulfil the requirements, data subject must be informed on all possible choices available to them, so that they can make a free choice of their volition. This is supported by EDPB Guideline 5/2020 which uses the term "real choice and control" [59] to describe the right that the data subject is entitled to. The "Obstruction" dark pattern deliberately hides certain choices to frustrate users into making a detrimental choice [60]. In the French DPA's deliberation concerning Facebook, the DPA remarked that users are unable to refuse cookies with the "same degree of simplicity" as accepting cookies [61]. Users had to go through the "Manage Data Settings" button, check that the slider buttons were disabled, then click the "Accept cookies" button to opt out [62]. This is counter-intuitive as the user had to "accept cookies" to refuse them. In other words, Facebook was attempting to obstruct users from opting out by introducing additional arguably confusing steps into the process. The French DPA's decision to impose an administrative fine and issue an injunction to remedy the opt out mechanism [63] demonstrates the effectiveness of the GDPR in curbing the use of Dark Patterns to obstruct users. Furthermore, in Orange România SA v ANSPDCP, Orange România required customers who refused consent to personal data processing to declare it in writing [64]. This presents a large obstruction as conclusion of a contract may now take a few days instead of just a few minutes if the customer were to consent to the processing. Thus, it is no surprise that the courts deemed such a practice to contravene the GDPR [65]. In closing, the definition of consent in the GDPR is a strong instrument that allows regulators to combat dark patterns that obstruct customers from refusing or withdrawing their consent.

55 Dir 2002/58/EU (n 13), para. 42

56 Information Commisioner's Office, *Monetary Penalty Notice* (2021) <https://ico.org.uk/media/action-weve-taken/mpns/4018348/we-buy-any-car-limited-mpn-20210913.pdf>, para. 31

57 Information Commisioner's Office (n 56), para. 72

58 reg 2016/679 (n 5), art. 4(11)

59 Article 29 Data Protection Working Party (n 54), pp. 5

60 Brignull and others, 'Deceptive Patterns' (n 15)

61 CNIL - French Data Protection Authority, *Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED* (2021) <https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf>, para. 90

62 CNIL - French Data Protection Authority (n 61), para. 88-89

63 CNIL - French Data Protection Authority (n 61), pp. 22

64 Case C-61/19 *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* ECLI:EU:C:2019:801, para. 50

65 *Orange Romania v ANSPDCP* (n 64), para. 52

7. Addressing Dark Patterns which exploit human psychology

When businesses are unable to obstruct customers from certain actions, they may instead resort to using Dark Patterns which exploit the human psychology to achieve their motives. "Nagging" continuously interrupts the customers to perform an action that is in the business's interest [66]. "Preselection" alters the default behaviour and relies on the psychological phenomenon where customers have a tendency to stick with the default option [67]. Humans have a finite amount of time and focus in a day, constant badgering as well as requiring customers to read and understand every form or dialog box will wear down even the most conscientious customer. "Confirmshaming" goes a step further by using emotions such as "guilt or shame" to nudge the customer towards a decision beneficial to the business [68].

Article 6(1)(f) of the GDPR protects the right of the customer to object to unnecessary personal data processing [69]. Article 21 of the GDPR is a *lex specialis* rule regulating direct marketing messages that directly prohibits processing for the purposes of "profiling" even if the marketing messages were eventually not sent [70]. In Nowegian DPA vs Komplett Bank ASA compliance order, the defendant was alleged to have repeatedly sent direct marketing emails to a customer despite the customer clearly opting out of such marketing [71]. Such behaviour is an example of "nagging" and Komplett Bank was attempting to repeatedly market to the customer in hope of wearing down the customer's resistance. Therefore, the continued processing for the purpose of sending marketing emails even after the customer has opted out contravenes Article 6(1)(f) and Article 21 of the GDPR [72] and Komplett Bank was ordered to remediate the non-compliant behaviours [73].

Recital 32 of the GDPR requires that consent be a "clear affirmative act", and prohibits inferring consent from pre-ticked boxes [74]. This is necessary to ensure unambiguous consent, and eliminate the possibly that the user scrolled past the box or did not notice it. In Bundesverband v Planet49, the court stated the importance of ensuring "active, rather than passive, behaviour" which is not present in a pre-ticked box [75]. As such, the court ruled that the use of a pre-ticked box does not constitute valid consent [76].

Lastly, Article 8 of the UCPD proscribes the use of aggressive practices that exert "undue influence" on the consumer's purchasing decision [77]. Item 30 of Annex I prohibits businesses from soliciting sales by lamenting that the "trader's

66 Brignull and others, 'Deceptive Patterns' (n 15)

67 Brignull and others, 'Deceptive Patterns' (n 15)

68 Brignull and others, 'Deceptive Patterns' (n 15)

69 reg 2016/679 (n 5), art. 6(1)(f)

70 reg 2016/679 (n 5), art. 21

71 Norwegian Data Protection Authority, *Final Decision - Compliance Order and Reprimand* (2021) <https://www.edpb.europa.eu/system/files/2022-02/no_2021-11_decisionpublic.pdf>, pp. 9

72 Norwegian Data Protection Authority (n 71), pp. 4 and 9

73 Norwegian Data Protection Authority (n 71), pp. 1

74 reg 2016/679 (n 5), recital. 32

75 Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Planet49 GmbH* ECLI:EU:C:2019:801, para. 52

76 *Bundesverband v Planet49* (n 75), para. 63

77 Dir 2005/29/EC (n 4), art. 8

78 Dir 2005/29/EC (n 4), annex. I, Item 30

job or livelihood will be in jeopardy" [78]. Hence the UCPD prohibits businesses from exploiting guilt to drive sales, and the "Confirmshaming" Dark Pattern will likely be contravening the UCPD.

8. Interplay and Overlapping of Legal Instruments

With so many different legal instruments regulating Dark Patterns, it is crucial to understand how they interplay and overlap, identify which is the *lex fori* in certain cases, so we can determine if there are *lacunae* in the legal framework. The UCPD has been described as a "safety net" [79] in a recent guidance released by the European Commission, as it pertains to all unfair business-to-consumer (B2C) commercial practices. The GDPR and ePrivacy directive is *lex specialis* regulation protecting personal data and privacy which may complement gaps in the UCPD where a non-profit or government entity processes personal data unfairly [80]. The CRD is *lex specialis* rule on pre-contractual information requirements. While the UCPD also applies to pre-contractual information, the CRD has more rigorous requirements including specifying after-sales services as well as duration of contract [81], hence the GDPR, CRD and ePrivacy Directive can be thought of as a safety harness which complements the coverage provided by the UCPD safety net. The e-Commerce Directive sets requirements on clearly identifying promotional offers and the qualifying conditions [82], which is not present in the UCPD. As for the MCAD, it regulates comparative advertising which is considered business-to-business (B2B) commercial practices, and fall outside the scope of the UCPD [83]. Hence, both the e-Commerce Directive and the MCAD can be visualized as its own safety net which does not overlap with the UCPD's safety net.

Considering the coverage provided by all the safety mechanisms, are there *lacunae* in the legislation where Dark Patterns can be abused? One possible *lacuna* lies in consumer-to-consumer (C2C) transactions [84]. An online auction seller could use confirmshaming to guilt consumers into purchasing his products. He could also possibly use trick wording when describing the condition of the product. However, most of the other Dark Patterns are likely not applicable since the seller is only able to modify limited product fields and cannot change the user interface of the auction website. Yet another *lacuna* exists in B2B sales since the MCAD only regulates marketing and advertising of competitors. Husovec supports this stance, arguing that Article 25 of the recently introduced DSA will alleviate the situation [85]. Procurement departments could *prima facie* fall prey to Dark Patterns when purchasing goods online. However, B2B sales often go through a more rigorous process with quotes obtained from multiple vendors, and negotiations before an agreement

79 European Commission, *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market* (2021) <https://commission.europa.eu/document/download/4f3285e1-54ed-402f-a9a7-d6769240b1aa_en>, para. 1.2.1

80 European Commission, *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market* (n 79), para. 1.2.1

81 Dir 2011/83/EU (n 11), art. 6(1)(m) and 6(1)(o)

82 Dir 2000/31/EU (n 14), art. 6

83 European Commission, *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market* (n 79), para. 1.1.2

84 MR Leiser and M Caruana Mireille, 'Dark Patterns: Light to be Found in Europe's Consumer Protection Regime' (2021) 10(6) Journal of European Consumer and Market Law 245

85 Martin Husovec, *Principles of the Digital Services Act* (1st, 2024), pp. 308

is reached [86]. Hence, it is unlikely that Dark Patterns has a noticeable impact on B2B sales.

All things considered, I believe the EU legal framework is moderately effective in tackling dark patterns. We have observed how the UCPD, GDPR, CRD and MCAD provides *de jure* protection against abuse of Dark Patterns. Through the numerous cases highlighted above, the defendants have been ordered to remediate non-compliant behaviour, reprimanded, served injunctions, and even fined for their actions. However, an OECD report noted that 60% to 90% of websites globally are using Dark Patterns [87]. Thus, we can deduce that the cases that have made it into the legal system are but a drop in the bucket compared to the volume of Dark Pattern abuse observed. The optimist might believe that the enforcement actions will have a strong deterrence effect as companies seek to avoid the legal, compliance and reputational costs should they receive a complaint for usage of Dark Patterns. However, the pessimist might argue that there is safety in numbers, and if majority of websites are utilizing Dark Patterns, the court system would never be able to effectively prosecute all offenders. This is supported by the recent fitness check document which surmised that the "number of consumer complaints remained at similar levels between 2008 and 2016", and there was no improvement in compliance to consumer law due to "insufficient enforcement" [88]. The volume of complaints also do not paint a full picture, since a portion of consumers may not be aware of Dark Patterns [89] or may have encountered those which exploit human psychology. Fortunately, the EU legal framework has a newly introduced ace up its sleeve - The Digital Services Act (DSA) [90].

9. The Way Ahead - Positioning the Safety Nets

The DSA acknowledges the impact of Dark Patterns by condoning its use directly in the legislation [91]. That, by itself, is not novel and provides only incremental protection above that provided by existing legislation [92]. However, the DSA is particularly shrewd in scoping its legislation to impose differing obligations based on the size of the platform [93]. Article 9 and 16 requires intermediaries and online platforms respectively to act against illegal content such as Dark Patterns [94]. Section 5 imposes stricter requirements on very large online platforms (VLOP) and search engines (VLOSE), requiring them to manage risk and perform independent audits [95]. VLOP

86 Gioconda Quesada and others, 'Impact of E-procurement on Procurement Practices and Performance.' (2010) 17(4) Benchmarking : an international journal <https://doi.org/10.1108/14635771011060576>, pp. 519

87 OECD (n 3), Annex C

88 European Commission, *Commission Staff Working Document - Fitness Check of EU consumer law on digital fairness* (2024) <https://commission.europa.eu/document/download/707d7404-78e5-4aef-acfa-82b4cf639f55_en?filename=Commission%20Staff%20Working%20Document%20Fitness%20Check%20on%20EU%20consumer%20law%20on%20digital%20fairness.pdf>, pp. 7

89 European Commission, *Commission Staff Working Document - Fitness Check of EU consumer law on digital fairness* (n 88), pp. 9

90 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1

91 reg 2022/2065 (n 90), para. 67

92 Husovec, *Principles of the Digital Services Act* (n 85), pp. 307

93 Ilaria Buri and Joris van Hoboken, 'The Digital Services Act (DSA) proposal: a critical overview' [2021] Digital Service Act (DSA) Observatory, pp. 18

94 reg 2022/2065 (n 90), art. 9 and 16

95 reg 2022/2065 (n 90), sect. 5

96 reg 2022/2065 (n 90), art. 33(1)

and VLOSE are platforms with more than 45 million monthly EU users [96], and together make up 91% of global search engine traffic [97] and 99% of global social media traffic [98] among others. With increased scrutiny on these nineteen services [99], it is no longer possible for them to hide among the crowd.

In one fell swoop, the DSA has shifted the EU legal framework from relying on complainants to proactive risk management and regular auditing that covers the vast majority of user traffic. To add on, the DSA has also shifted some of the costs of compliance onto platforms by mandating internal compliant handling systems [100] and charging a supervisory fee [101]. Instead of weaving ever larger safety nets, the EU has strategically positioned safety nets in locations where the vast majority of users are likely to fall. *De minimis non curat lex*. We do not have to go after all websites that are using Dark Patterns, but just the top websites that account for the majority of user traffic. The DSA has greatly increased the *de facto* effectiveness of combating Dark Patterns, with the first such case against X for allegedly using the "Blue checkmark" in a deceptive manner which could fall under the "Fake social proof" Dark Pattern [102]. Husovec remarked that the "carve-out in Article 25(2) has an uncertain scope" [103]. Article 25(2) excludes practices which fall under UCPD and GDPR from the ambit of Article 25(1) [104]. Given that the "Blue checkmark" is likely to have commercial implications such as influencing purchasing decisions, it could fall under the scope of the UCPD. It will be interesting to observe the court's interpretation on Article 25(2).

10. Conclusion

We have attempted to categorize Dark Patterns into five different categories, those that hide information, sow confusion, present false information, obstruct users and finally those that exploit human psychology. Through analysis, we have determined that the EU legal framework has effective legislation that forbids usage of all types of Dark Patterns. Based on the various case judgments and enforcement notices, the courts are successful at protecting the rights of consumers against the businesses. However, based on empirical data, it has been suggested that the use of Dark Patterns is rampant and the cases that come before the court may only be the tip of the iceberg. Fortunately, with the introduction of the DSA, regulators are able to hold large platforms to higher standards and greater scrutiny. Given that these large platforms account for majority of EU internet traffic, the future of EU consumer protection just got brighter.

---

97 Tiago Bianchi, 'Market share of leading desktop search engines worldwide from January 2015 to January 2024' (*Statista*, 22 May 2024) <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/> accessed 6 December 2024

98 areppim AG, 'Mobile social media Percent Market Share Worldwide (As of October 2017)' (*areppim AG*) <https://stats.areppim.com/stats/stats_socmedia_mobixsnapshot.htm> accessed 6 December 2024

99 European Commission, 'Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines' <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413> accessed 25 April 2023

100 reg 2022/2065 (n 90), art. 20

101 reg 2022/2065 (n 90), art. 43

102 European Commission, *Commission sends preliminary findings to X for breach of the Digital Services Act* (2024) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_3761/IP_24_3761_EN.pdf>

103 Martin Husovec, 'The DSA Newsletter #6' (26 September 2024) <https://husovec.eu/2024/09/the-dsa-newsletter-6/> accessed 15 December 2024

104 reg 2022/2065 (n 90), art. 25(2)

Bibliography

Cases

Case C-611/14 *Anklagemyndigheden v Canal Digital Danmark A/S* ECLI:EU:C:2016:800.

Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Planet49 GmbH* ECLI:EU:C:2019:801.

Case C-562/15 *Carrefour Hypermarchés SAS v ITM Alimentaire International SASU* ECLI:EU:C:2017:95.

Case C-61/19 *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* ECLI:EU:C:2019:801.

Case C-371/20 *Peek & Cloppenburg KG v Peek & Cloppenburg KG* ECLI:EU:C:2021:674.

Case T-1030/23 *Tiktok Technology v European Data Protection Board* (ECJ).

Viagogo AG v Competition and Markets Authority [2019] EWHC 1706.

Legislation

Directive 2000/31/EC Of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)) [2002] OJ L201/1.

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 and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22.

Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising [2006] OJ L376/21.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Counci [2011] OJ L304/64.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

Reports

Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (2017) <https://ec.europa.eu/newsroom/article29/items/623051>.

CNIL - French Data Protection Authority, *Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED* (2021) <https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf>.

Competition and Markets Authority, *Transparency of heating oil price comparison websites* (2011) <https://www.gov.uk/cma-cases/transparency-of-heating-oil-price-comparison-websites> accessed 10 November 2024.

— *CMA secures changes to Xbox subscription practices* (2022) <https://www.gov.uk/government/news/cma-secures-changes-to-xbox-subscription-practices> accessed 8 November 2024.

European Commission, *Expedia enforcement action* (2020) <https://commission.europa.eu/system/files/2020-12/factsheet-expedia_enforcement_action_1.pdf> accessed 10 November 2024.

— *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market* (2021) <https://commission.europa.eu/document/download/4f3285e1-54ed-402f-a9a7-d6769240b1aa_en>.

— *Commission sends preliminary findings to X for breach of the Digital Services Act* (2024) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_3761/IP_24_3761_EN.pdf>.

— *Commission Staff Working Document - Fitness Check of EU consumer law on digital fairness* (2024) <https://commission.europa.eu/document/download/707d7404-78e5-4aef-

acfa-82b4cf639f55_en?filename=Commission%20Staff%20Working%20Document%20Fitness%20Check%20on%20EU%20consumer%20law%20on%20digital%20fairness.pdf>.

European Data Protection Board, *Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)* (2023) <https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf>.

High Court of Justice, *Competition and Markets Authority and Viagogo AG - Enforcement Order* (2018) <https://assets.publishing.service.gov.uk/media/5bffe2afe5274a0fae2c5397/CMA_v_Viagogo_Order_27.11.pdf> accessed 10 November 2024.

Information Commisioner's Office, *Monetary Penalty Notice* (2021) <https://ico.org.uk/media/action-weve-taken/mpns/4018348/we-buy-any-car-limited-mpn-20210913.pdf>.

Norwegian Data Protection Authority, *Final Decision - Compliance Order and Reprimand* (2021) <https://www.edpb.europa.eu/system/files/2022-02/no_2021-11_decisionpublic.pdf>.

Books

Brignull H, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (1st, 2023).

Husovec M, *Principles of the Digital Services Act* (1st, 2024).

Articles

Buri I and Hoboken J van, 'The Digital Services Act (DSA) proposal: a critical overview' [2021] Digital Service Act (DSA) Observatory.

Leiser MR and Caruana Mireille M, 'Dark Patterns: Light to be Found in Europe's Consumer Protection Regime' (2021) 10(6) Journal of European Consumer and Market Law 245.

OECD, 'Dark commercial patterns' (2022) 336 OECD Digital Economy Papers <https://doi.org/10.1787/44f5e846-en>.

Quesada G and others, 'Impact of E-procurement on Procurement Practices and Performance.' (2010) 17(4) Benchmarking : an international journal <https://doi.org/10.1108/14635771011060576>.

Secondary Sources

areppim AG, 'Mobile social media Percent Market Share Worldwide (As of October 2017)' (*areppim AG*) <https://stats.areppim.com/stats/stats_socmedia_mobixsnapshot.htm> accessed 6 December 2024.

Bianchi T, 'Market share of leading desktop search engines worldwide from January 2015 to January 2024' (*Statista*, 22 May 2024) <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/> accessed 6 December 2024.

Brignull H and others, 'Deceptive Patterns' (25 April 2023) <https://www.deceptive.design/types> accessed 2 November 2024.

— 'Deceptive Patterns - Hall of Shame' (25 April 2023) <https://www.deceptive.design/hall-of-shame> accessed 2 November 2024.

European Commission, 'Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines' <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413> accessed 25 April 2023.

Husovec M, 'The DSA Newsletter #6' (26 September 2024) <https://husovec.eu/2024/09/the-dsa-newsletter-6/> accessed 15 December 2024.

Santos C and Rossi A, 'The emergence of dark patterns as a legal concept in case law' (31 July 2023) <https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept> accessed 8 November 2024.