Dark Patterns, Enforcement, and the emerging Digital Design Acquis --

Manipulation beneath the Interface

By Dr M.R. Leiser (Mark) and Dr Cristiana Santos

Abstract

The term 'dark patterns' is commonly used to describe manipulative techniques implemented into the user interface of websites and apps that lead users to make choices or decisions that would not have otherwise been taken. Legal academic and policy work has focussed on establishing classifications, definitions of dark patterns, constitutive elements, and typologies of dark patterns across different fields. Regulators have responded to this issue with several enforcement decisions related to data protection and privacy violations, and with rulings protecting consumers. Accordingly, this article analyses the appropriateness of regulatory oversight of designers and platforms that deploy dark patterns inside digital technologies. By further analysing design techniques, we conclude this type of deceptive design is inappropriately attributed to the user interface when some patterns are embedded in the system architecture. With this in mind, the article also analyses the emerging *digital design acquis* of the European Union. The Digital Markets Act and Digital Services Act, the proposals for a new Data Act and AI Act are critiqued for suitability of regulating deceptive design over the entirety of, what we coin, the deceptive design visibility spectrum.

Keywords: dark patterns, deceptive design, manipulative design, digital design acquis, regulation, law, user interface, data protection, consumer protection, HCI.

Introduction[1]

'Dark patterns'[2] or deceptive design refer to design practices that manipulate[3] or exploit users to achieve specific outcomes, often at the expense of their autonomy, judgments, decision-making, or choices.[4] These patterns may range from subtle nudges to overtly coercive tactics that deceive or trick users into taking specific actions that benefit the platform or service provider. The use of dark patterns has become a growing concern. The response to dark patterns has evolved from theoretical problem-based academic work[5] and behavioural studies[6] to active enforcement by regulatory bodies worldwide.[7] The amalgamation of these results has yielded a preliminary framework for policy-oriented interventions delineating the perils posed by dark patterns and associated deceitful design techniques. For example, when the EU's Consumer Protection Co-operation (CPC) Network swept 399 retail websites and apps for dark patterns, nearly 40% of online shopping websites relied on manipulative practices to trick and exploit consumers' vulnerabilities. Various regulatory bodies, including the US Federal Trade Commission (FTC)[8], the UK Competition and Market Authority (CMA)[9], the European Commission[10], the European Data Protection Board (EDPB),[11] and the Organisation for Economic Co-operation and Development (OECD)[12], have issued high-profile policy guidance on distinct varieties of dark patterns that exhibit significant

[1] The authors would like to thank Harry Brignull, the design ethicist who coined the term 'dark patterns', for his incredibly valuable assistance on our enforcement database and helping us understand the intricacies of design principles. We also extend heartfelt gratitude to our wonderful research assistant, Kosha Doshi. Her work compiling and analysing the enforcement rulings referred to in this paper has been invaluable.

[2] We use the terms 'dark patterns' and 'deceptive design' interchangeably.

[3] Manipulation consists in a form of influence that subverts the user's capacity to make a conscious decision. For the differentiation between different types of manipulation, we refer to Susser, Daniel, Beate Roessler, and Helen Nissenbaum. 2019. 'Technology, Autonomy, and Manipulation.' Internet Policy Review 8 (2). https://doi.org/10.14763/2019.2.1410.

[4] (UK Competition and Markets Authority (CMA), the United States's Federal Trade Commission (FTC), The Netherland's Autoriteit Consument & Markt (ACM) and several data protection authorities)

[5] Christoph Bösch and others, 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' (2016) 4(4) Proceedings on Privacy Enhancing Technologies https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf; ; Lothar Fritsch and others, 'Privacy Dark Patterns in Identity Management' [2017] 0(0) Lecture Notes in Informatics (LNI) 93;ce under the Unfair Commercial Practices Directive' (2022) https://osf.io/preprints/socarxiv/7dwuq/ accessed 11 April 2023.

[6] European Commission, Directorate-General for Justice and Consumers, Francisco Lupiáñez-Villanueva and others, Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation: Final Report (Publications Office of the European Union 2022) https://data.europa.eu/doi/10.2838/859030 accessed 15 March 2023.

[7] See the Leiser, Santos, and Doshi (2023), Dark Patterns Enforcement Database (Forthcoming).

[8] FTC, Bringing Dark Patterns to Light (2022) https://www.ftc.gov/system/files/documents/reports/bringing-dark-patterns-to-light/bringing_dark_patterns_to_light.pdf accessed 16 March 2023.

[9] Consumer and Markets Authority's Online Choice Architecture Discussion Paper (2022) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf accessed 16 March 2023.

[10] Behavioural study on unfair commercial practices in the digital environment (European Commission, 2022) https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418 accessed 16 March 2023.

[11] The European Data Protection Board (EDPB) has also taken steps to address dark patterns by publishing guidelines on the subject. The guidelines define dark patterns as "features of interface design crafted to trick users into making choices that they might not otherwise make." The guidelines go on to explain that dark patterns can be used to "subvert end-users cris tautonomy, decision-making, or free choice" and can be found in various forms, including misleading information, pre-selected choices, and confusing language - Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en accessed 15 March 2023.

[12] Dark commercial patterns (OECD, 2021) https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en accessed 16 March 2023.

overlap with definitions put forth in academic literature.[13] Additionally, in 2022, the German Federal Financial Supervisory Authority (BaFin) enacted a mandate forbidding dark patterns in trading applications or portals.[14]

The present means of studying deceptive design and its legal implications centres around a descriptive and classificatory approach to identifying malicious strategies and assessing their legality within the confines of specific legislative instruments. In contrast, this article undertakes a regulatory analysis of dark patterns from EU data protection, consumer, competition and platform regulation perspectives to elucidate the common themes that emerge from enforcement decisions. The attainment of general deterrence requires the execution of four essential steps, including enforcement, detection, penalties, and publicity. In light of this, the scrutiny of regulatory cases that can be classified as dark patterns holds significant significance and marks the first attempt to investigate this area of study. This article conducts an enforcement analysis of dark patterns, specifically those that are presently being tackled by three critical pieces of legislation, namely the General Data Protection Regulation (GDPR)[15], the ePrivacy Directive (ePD)[16], and the Unfair Commercial Practices Directive (UCPD)[17], that are working to establish legal standards for transparent and fair data processing and marketing practices.

Part 1 analyses these decisions, concluding that most enforcement decisions across the EU primarily deal with user interface techniques, such as preselection, forced continuity, complicated refusal mechanisms, the prominence of certain choices, bundling practices and nefarious information practices. More hidden techniques include informational practices, such as ambiguous language, the absence or lack of accessibility of information, and system architecture practices, which refer to manipulative techniques that are invisible to users but can be identified through technical means. Our examination reveals a tendency among regulators to focus exclusively on "visible" dark patterns present in online user interfaces and experiences while neglecting the more insidious and covert patterns embedded within system architectures. We then advance this discussion in two ways: first, by proposing a three-tier visibility threshold for dark patterns:

---

[13] J. Luguri and L. Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13 Journal of Legal Analysis 43, 44; A. Mathur, J. Mayer and M. Kshirsagar, 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods' (Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Article no. 360, 2021), 3 at https://doi.org/10.1145/3411764.3445610; A. Mathur, G. Acar, M. Friedman, E. Lucherini, J. Mayer, M. Chetty and A. Narayanan, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human Computer Interaction 81, 82; C. Gray, C. Santos, N. Bielova, M. Toth and D. Clifford, 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' (Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Article no. 172, 2021), 1 at https://doi.org/10.1145/3411764.3445779; Midas Nouwens and others, 'Dark Patterns After The GDPR: Scraping Consent Pop-Ups And Demonstrating Their Influence' (Association for Computing Machinery (ACM 2020)) https://dl.acm.org/doi/pdf/10.1145/3313831.3376321?casa_token=fDsPakcJwQUAAAAA%3A5p2usbRAr38SO8uMnfoX5xBE9-hh_JVVsak59KKRzVdhBZpmrjh2hY5Ac_vouC447mtHvU6UcxDj;[Author Unknown], 'Dark Patterns: Submission By Design?' (Medium, 2021) https://uxdesign.cc/dark-patterns-submission-by-design-6f61b04e1c92; Mireille M Caruana and M R Leiser, 'Dark Patterns: Light to be Found in Europe's Consumer Protection Regime' (2021) 10(6) Journal of European Consumer and Market Law; Mark R Leiser, 'Dark Patterns: The Case for Regulatory Pluralism between the European Union's Consumer and Data Protection Regimes' in Research Handbook on EU Data Protection Law (Edward Elgar Publishing 2022) 240; Mark Leiser and W T Yang, 'Illuminating Manipulative Design: From "Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive' (2022); Clifford, D. (2017) and Lior Strahilevitz et al., Subcommittee report: Privacy and data protection, Stigler Center Committee for the Study of Digital Platforms 22-23 (2019); Leiser, M. R. (2022). Dark patterns: The case for regulatory pluralism between the European Unions consumer and data protection regimes. In Research Handbook on EU Data Protection Law (pp. 240-269). Edward Elgar Publishing; Leiser, M. R., & Caruana, M. (2021). Dark Patterns: Light to be found in Europe's Consumer Protection Regime. Journal of European Consumer and Market Law, 10(6), 237-251; Leiser, M., & Yang, W. T., 'Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive' (2022) https://osf.io/preprints/socarxiv/7dwuq/ accessed 11 April 2023.

[14] Bundesanstalt für Finanzdienstleistungsaufsicht, 'Dark Patterns in Trading Apps - Expertenartikel' (BaFin, 21 November 2022) https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2022/meldung_2022_11_21_Dark_Patterns_in_TradingApps_Experten.html accessed 15 March 2023.

[15] General Data Protection Regulation (EU) 2016/679.

[16] Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the ePrivacy Directive').

[17] Unfair Commercial Practices Directive (EU) 2005/29/EC

Visible dark patterns constitute open and overtly manipulative design practices that exert readily recognisable effects on user decision-making, and that are more easily recognizable, such as deliberately obscuring or concealing an unsubscribe button.

In contrast, ***darker*** patterns are more subtle and elusive, utilising persuasive design techniques to exploit user vulnerabilities or biases for specific purposes, such as hidden fees or misleading advertising. Users only realise the consequences of these patterns after the fact.

The ***darkest*** patterns are intricate and either a) deterministic - relying on sophisticated coding or architecture to achieve specific outcomes, or b) stochastic (non deterministic) patterns. In the latter,- where the system is a black box and nobody can explain precisely why the system output what it did, and the system may give different outputs to the same inputs (e.g. ML, learning systems, other statistical stuff). Unlike visible and darker patterns, these classifications cannot be intuited from a flow chart.

Part 2 focuses on the role of designers and developers in controlling deceptive design practices built into the system architecture of digital systems. Although designers must balance the needs of clients, businesses, and users to prevent deceptive UI/UX services, they must also take responsibility to avoid dark patterns. Current legislative initiatives only regulate the online graphical interface of digital systems and fail to consider surface-free interactions and their potential for manipulative design practices. Regulatory oversight should, therefore, include the entire system architecture to ensure that digital systems are designed in a legally compliant way. The European Union (EU) has demonstrated its commitment to addressing the issue of dark patterns through a series of regulations, including the Digital Services Act[18], Digital Markets Act[19], Data Act Proposal[20], and AI Act Proposal[21]. Incorporating the term into Guidance Documents[22] and Codes of Conduct[23] and developing these regulations highlights the EU's growing recognition of the adverse effects of dark patterns. Notably, under the leadership of the European Commissioner for Justice and Consumer Protection, Didier Reynders, the EU Commission has announced its intention to prioritise the regulation of dark patterns in its 2023 mandate.[24] The EU's comprehensive *digital design acquis* indicates that the dark pattern rules will extend beyond any individual legislation and will likely be enforced across sectors, encompassing data protection and consumer law alongside platform regulation.

Accordingly, **Part 3** analyses the EU's recent and forthcoming regulatory approaches, concluding that the GDPR, ePD and the UCPD sufficiently address ***visible*** and ***darker*** patterns, but has not adequately addressed the ***darkest*** patterns in System Architecture. However, the EU has also addressed dark patterns and deceptive design practices through various legislative measures. For instance, the Digital Services Act (DSA), the Digital Markets Act (DMA) impose new obligations on online platforms and digital service providers, such as transparency and user choice requirements. It seeks to ensure fair competition in the digital economy by regulating the behaviour of dominant online platforms. These laws establish legal standards for transparency and fair competition, which can help regulate dark patterns. Additionally, the AI Act proposal recognises the potential harm caused by dark patterns. It sets clear legal requirements for developing and deploying artificial intelligence systems, including transparency, accountability, and human oversight. Similarly, the proposed Data Act establishes new data governance frameworks and standards for using personal data, including transparency, consent, and accountability

[18] 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)

[19] Regulation (EU) 2022/1925 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)

[20] Regulation on harmonised rules on fair access to and use of data (Data Act).

[21] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

[22] 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 (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021XC1229(05)&from=EN

[23] Center for Humane Technology, 'Design Guide', Humane Technology (accessed 16 March 2023) https://www.humanetech.com/designguide.

[24] Dark patterns, online ads will be potential targets for the next Commission, Reynders says, https://www.euractiv.com/section/digital/interview/dark-patterns-online-ads-will-be-potential-targets-for-the-next-commission-reynders-says/

requirements. It will likely play a significant role in regulating dark patterns, particularly collecting, processing, and using personal data. Thus, the EU's recent approach to regulating platforms and digital technologies (the Digital Services Act, the Digital Markets Act, the Data Act proposal, the Proposal for an Artificial Intelligence Act) are critiqued as part the EU's emerging *digital design acquis*.

In the final part, we further critique the suitability of the current regulatory regime, concluding that *digital design acquis* in its current form is insufficient to regulate dark patterns across the entire spectrum of visibility. Theoretically, the EU should provide a comprehensive regulatory framework for regulating dark patterns and deceptive design practices. The GDPR and ePD, the UCPD, the AI Act proposal, the DSA, the DMA, and the proposed Data Act are meant to establish legal standards for transparency, fairness, and accountability, which should regulate dark patterns across the entire spectrum of visibility. However, the effectiveness of the regulatory response will largely depend on the creative interpretation of several provisions lest the entire *acquis* is deemed insufficient. Accordingly, **Part 4** provides guidance on how regulators should tackle dark patterns in any enforcement actions across the entirety of the EU's emerging *digital design acquis.*

Part I: Enforcement against Dark Patterns

Effective enforcement is an essential component in regulating dark patterns, ensuring that businesses and service providers conform to legal standards of transparent, fair, and ethical design practices. The General Data Protection Regulation (GDPR), the ePrivacy Directive (ePD), and the Unfair Commercial Practices Directive (UCPD) collectively provide a robust regulatory framework for overseeing dark patterns across platforms, apps, and websites. Consumer and data protection authorities have diligently fulfilled their enforcement responsibilities, initiating legal actions under relevant laws against dark patterns without explicitly designating them as such. In the following sections, we present our analysis of the enforcement decisions made by data protection and consumer regulators.[25] We analyse the decisions per legal domain, separating them into data protection (in section one) and consumer law (in section 2). We select the practices that may relate to known dark pattern taxonomies.[26] Our analysis of regulatory decisions reveals that deceptive design exists on a spectrum, ranging from visible dark patterns, which are readily observable by any stakeholder analysing or auditing them (e.g., regulators, policymakers), to less visible "darker" patterns, and ultimately to completely invisible "darkest" patterns. Therefore, we present our findings from the collected decisions according to this visibility spectrum. Table 1 illustrates the distribution of regulatory consumer and data protection cases based on the visible spectrum and per dark pattern type.

Enforcement from a data protection perspective

Our thorough examination of regulatory decisions indicates that although the GDPR and ePrivacy Directive does not expressly mention dark patterns, these legislative frameworks play a fundamental role in their governance. Specifically, entities that rely on consent to process personal data under the GDPR or to acquire consent for cookies or marketing communications under the ePrivacy Directive may utilise dark patterns when soliciting such consent.

---

[25] To comprehensively assess the scope and nature of enforcement, we gathered regulatory decisions from multiple sources, including data protection authorities (DPAs), consumer protection agencies, and competition authorities until the end of January 2023. From a data protection standpoint, we consulted the GDPRhub repository (https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub), which provides cases in original languages and automated English translations. We utilised DeepL and Google Translate tools to ensure clarity when these translations were insufficiently accurate. Though we analysed around 118 regulatory decisions, we did not aim to account for all regulatory decisions exhaustively. Due to the qualitative nature of this analysis, we do not provide quantified numbers of how many decisions relate to dark patterns.

[26] The labelling of certain practices identified in the decisions as dark patterns relied upon the author's expertise in data protection and consumer laws and on the lawfulness of dark patterns. The authors labelled such practices using the OECD taxonomy of dark patterns, and resorted to the high-level categories of dark patterns described therein, cf. OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

Visible dark patterns

The phenomenon of "visible dark patterns" is characterised by the inclusion of manipulative design features in the user interface, such as “pre-checked options”, “bundling or tying practices”, “obstructive refusal and withdrawal options”, “wrong language”, and “forced actions”. These patterns are easily recognisable to non-experts and have an observable impact on user decision-making. Notably, the most prevalent dark patterns involve preselection, obfuscation of refusal and withdrawal mechanisms, and bundled practices.

“Pre-checked boxes”[27] have decreased in recent years due to explicit judicial prohibitions,[28] and further guidelines from the European Data Protection Board (EDPB)[29] and Data Protection Authorities (DPAs).[30] Instead, users are presented with default options for consent[31] for data sharing with third parties under advertising targeting or commercial communication. These practices are referred to as “preselection” practices, or *defaults*, since users are tricked or forced into sharing more personal information than desired.[32]

Several decisions report the use of “bundling or tying practices” used in tracking and non-tracking scenarios. Decisions refer to practices that force users to accept the terms and conditions of a service together with privacy policies in bulk and simultaneously to use an app.[33] In some cases,[34] the use of a certain service required users to consent to data processing. Users may also be subjected to e-marketing without choice.[35] Users are also asked to consent for multiple unrelated purposes (including advertising), without any meaningful granular choice,[36] or are asked to consent to the processing of tracers that serve several and different purposes.[37] Such practices infringe on users' free and specific consent and are considered dark patterns of "forced action"[38] as users are tricked or forced into sharing more personal information than desired.

The decisions made by the DPA reveal instances of “obstructive refusal and withdrawal options”. These decisions refer to cases where users had to perform a high number of actions pursuant to deactivating or disabling their settings[39] and selecting more privacy-preserving options(without advertising being enabled). Several cases[40] reported how cumbersome or impossible it was to reject non-necessary trackers, such as third-party advertising

---

[27] Recital 32 GDPR explicitly forbids pre-checked boxes.

[28] Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverb ̈ande – Verbraucherzentrale Bundesverband eV v Planet49 GmbH.

[29] European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. 2020

[30] All DPA guidelines on consent confirm that consent obtained through pre-checked options renders consent invalid.

[31] French DPA vs Apple, 2022; Belgian DPA vs Rossel & Cie, 2022; French DPA vs Google LLC, 2019; Belgian DPA vs Roularta Media Group, 2022; Belgian DPA vs Y, 2019; Danish DPA vs DMI, 2020; Spanish DPA vs Caixabank, 2019; UK DPA vs Money Hive Limited (TMHL), 2022; Spanish DPA vs Hospital Recoletas Ponferrada, 2022.

[32] OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

[33] French vs Google LLC, 2019; Finish DPA vs Polar Oy.

[34] Norway DPA vs Grindr LLC, 2021; Latvian DPA vs SIA DEPO DIY, 2022; Finish DPA vs Polar Oy, 2022; UK DPA vs Colour Car Sales Limited, 2021; French DPA vs Google LLC, 2020; Spanish DPA vs Add Event Staff, S.L., 2020; Spanish DPA vs Vueling Airlines S.A., 2019; Spanish DPA vs Bodegas Dinastía, S.L., 2020; Belgian DPA vs youronlinechoices, 2022.

[35] Spanish DPA vs Add Event Staff, S.L., 2020; UK DPA vs Colour Car Sales Limited, 2021; Hungarian DPA vs service provider (incognito), 2022.

[36] Art. 4(11), 7(3) GDPR

[37] French DPA vs Microsoft, 2022.

[38] OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

[39] French DPA vs Apple, 2022;

[40] French vs Facebook Ireland Limited, 2021; Spanish DPA vs Happy Friday, S.L., 2022; Spanish DPA vs Lia's Clothes, 2021; Spanish DPA vs Ramona Films S.L, 2022; Spanish DPA vs Iberia, 2020; Spanish DPA vs Marbella Resorts, 2021; Spanish DPA vs Radio Popular, 2021; Spanish DPA vs FDM, 2020; Spanish DPA vs FurnishYourSpace, 2020; Spanish DPA vs Twitter, 2021; Spanish DPA vs The Washpoint SL, 2020; Spanish DPA vs The Washpoint SL, 2020; Spanish DPA vs Facua, 2020; Danish DPA vs DGU Erhverv A / S, 2020; Danish DPA vs JAVA, 2020; Spanish DPA vs X, 2020; Finish DPA vs Traficom, 2020; French DPA vs Tiktok 2022; Danish DPA vs DMI, 2020; Spanish DPA vs Miguel Ibáñez Bezanilla, S.L., 2020; Spanish DPA VS Canary Click Consulting website, 2020; Belgian DPA vs Toerisme Vlaanderen, 2O22; Norway DPA vs Grindr LLC, 2021; French DPA vs Microsoft, 2022; Belgian DPA vs Youronlinechoices, 2022.

trackers. Examples illustrate a lack of control panels for rejecting consent; inadequate options for declining at the second layer of a cookie banner; the need to configure browser settings or visit third-party websites to deny for each partner separately). Other cases[41] report that data subjects did not have the possibility to withdraw consent regarding cookies, or cases[42] wherein users could not withdraw consent as easily as it was given (e.g. through the use of a link in the commercial information; demanding to provide the reason for withdrawing consent). Some decisions[43] report that objections to unsolicited marketing were also hindered by the difficulty of communicating the right to object to data processing, which was necessary through multiple direct marketing channels, or requiring users to contact the company or visit a physical store. Few cases[44] refer to the fact that some companies did not provide an account cancellation option for their website or app. Such sanctioned practices fall under the dark patterns category named "obstruction",[45] denoting asymmetry in ease of giving consent versus rejecting/withdrawing.

The scenario of adopting a "wrong language" has been observed in certain instances where the data protection information of a website is not provided in the official language of the country where users live.[46] If users do not master the language in which the privacy policy information is given, they will not be able to easily read it and therefore likely to not be aware of how data is processed, which is especially severe when a website addresses children. This practice has been named by the EDPB as "language discontinuity"[47] type of dark pattern.

Our analysis found some cases wherein data controllers (and its commercial third-party partners with whom personal data was shared) "repeatedly prompted users with unsolicited promotional and advertising messages"[48] that were sent through several means (texting, emails, automated phone calls) after users had objected to such processing, or even without the data subject's consent. In one case, the regulator referred to such practice as a "persistent and disturbing sense of interference in their sphere of privacy due to these practices, which are often accompanied by behaviour that complainants perceive as not only invasive but also particularly aggressive."[49] This repetitive and obstructive communication disrupts users and infringes the principles of lawfulness and fairness. Moreover, these behaviours might entail the dark patterns of "nagging".[50]

Darker dark patterns

Darker dark patterns refer to covert practices that are not immediately discernible to users, necessitating further scrutiny by regulatory authorities and expert auditors. Design choices involving "complex information that is hard to understand", "misleading practices", "absence or obscurity of relevant data", "forced practices", and "fragmented data protection information" represent darker, less visible and less detectable dark patterns.

Certain decisions are reported to be challenging for users due to the "complex nature of the information" provided, even though the GDPR requirement for data protection information to be clear, concise, transparent, and easily accessible using plain language[51] is essential to enable users to make informed choices. For instance, certain

---

41 Spanish DPA vs X website, 2022.

42 Belgian DPA vs Roularta Media Group, 2022; Spanish DPA vs X, 2019; Polish DPA vs ClickQuickNow Sp. z o, 2019;

43 Belgian DPA vs Telenet, 2021; Italian DPA vs Wind Tre SpA, 2020; UK DPA vs Colour Car Sales Limited, 2021.

44 Spanish DPA vs Cooltra Motosharing S.L.U., 2019.

45 OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

46 French DPA vs Tiktok 2022; Austrian DPA vs Co Material GmbH, 2021;Spanish DPA vs AAA Just Landed S.L, 2019.

47 EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en accessed 15 March 2023.

48 Italian DPA vs Enel Energia Spa, 2021; UK DPA vs American Express ('AMEX'), 2021; Spanish DPA vs BORJAMOTOR, S.A., 2000; Belgian DPA vs National Service for the Promotion of Childcare products, 2021; Spanish DPA vs Banco Bilbao Vizcaya Argentaria, SA, 2020; Belgian DPA vs Y VZW, 2020.

49 Italian DPA vs Enel Energia Spa, 2021; UK DPA vs We Buy Any Car Limited, 2021; Italian DPA vs Wind Tre SpA, 2020; Norway DPA vs Komplett Bank ASA, 2021; UK DPA vs Unite the Union, 2021.

50 OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

51 Article 12, GDPR.

names[52] that are given to options were framed as unclear (e.g. “manage data settings” button, or “we use cookies to optimize the users' experience); other cases report lack of clarity and understandability of essential information that does not allow users to sufficiently understand the particular consequences of the processing for them[53] on the pursued description of purposes, data controller, collected data, the legal basis for certain purposes, retention periods, joint controllers, etc.[54] Other decisions report that the cookie banner only offered generic information[55], or the privacy policy was vague.[56] Such practices can be related to the dark pattern of “obstruction”.

“Misleading practices” were also observed in the analysed decisions. These include incorrectly categorization of third-party cookies as technically essential, and consequently, when users unchecked the relevant boxes or clicked "reject all," non-essential cookies remained[57]; or the case of company used some cookies for a purpose which was not listed in its privacy policy [58], or the use of a cookie serving several purposes.[59] Other decisions denounce that data protection information was provided in very small print, barely legible.[60] Moreover, cases expose that privacy policies state misleading information[61] (e.g. stating that personal data would only be used for “strictly necessary purposes”, but also that marketing was included in data processing.[62] Other cases divulges the use of some cookies for a purpose which was not listed in its privacy policy[63]. Finally, it was denoted the use of misleading and complicated language[64] (for example, whilst the identity and contact details of the data controller were provided in the privacy notice, they were included under a misleading title, giving the impression that they were provided for a business purpose). These practices described can be associated with dark patterns of "obstruction," "sneaking," and "misleading information." Such practices can limit user autonomy and control, making informed decision-making difficult.

Some “design choices hide” data protection information, making it difficult to access and violating Article 12 of the GDPR. These practices can be associated with dark patterns of "hidden information" and "sneaking." Cases report instances where users are not informed about data processing purposes, third-party recipients, and data sharing, resulting in insufficient information on privacy or cookie policies, making it difficult for users to make informed decisions. In particular, the cases report to practices where users not informed about data processing purposes (and how to reject them);[65] and users not informed about third party recipients with whom data was shared with (for advertising purposes).[66]

“Forced practices” demonstrating user consent exploitation and personal data manipulation were sanctioned when personal data is processed before consent is given,[67] and aso when non-essential trackers (such as advertising and

[52] French vs Facebook Ireland Limited, 2021; Spanish DPA vs FurnishYourSpace, 2020.

[53] Irish DPA vs Whatsapp Ireland Limited, 2021; French DPA vs Google LLC, 2020; French DPA vs Google LLC, 2020; Hungarian DPA vs Magyar Éremkibocsátó Kft., 2022; Belgian DPA vs National Service for the Promotion of Childcare products, 2021; Portuguese DPA vs INE, 2021; Italian DPA vs Wind Tre SpA, 2020; Belgian DPA vs Toerisme Vlaanderen, 2O22; Belgian DPA vs Y VZW, 2020; Spanish DPA vs Facua, 2020.

[54] Danish DPA vs DMI, 2020.

[55] Spanish DPA vs FDM, 2020; Spanish DPA vs Bodegas Dinastía, S.L., 2020.

[56] Spanish DPA vs Happy Friday, S.L., 2022; UK DPA vs Emailmovers Limited, 2021;Swedish DPA vs Klarna Bank AB, 2022; Belgian DPA vs Y Housing Company, 2020; Czech DPA vs Television operator, 2021.

[57] Spanish DPA vs Vueling Airlines S.A., 2019.

[58] French DPA vs Carrefour Group, 2020.

[59] French DPA vs Microsoft, 2022.

[60] Hungarian DPA vs Magyar Éremkibocsátó Kft., 2022.

[61] Hungarian DPA vs Infotv, 2022; Belgian DPA vs Toerisme Vlaanderen, 2O22;Spanish DPA vs Iberia, 2020.

[62] Spanish DPA VS Canary Click Consulting website, 2020; Spanish DPA vs Esclora Proyectos, 2020.

[63] French DPA vs Carrefour Group, 2020.

[64] Spanish DPA vs FurnishYourSpace, 2020; Spanish DPA vs Facua, 2020.

[65] Luxembourg DPA vs Amazon, 2021;Spanish DPA vs Grupo Bandera Catalana, 2018; Spanish DPA vs Iweb Internet Learning, S.L, 2020.

[66] Norway DPA vs Grindr LLC, 2021.

[67] Italian DPA vs Uber Italy srl, 2022; Spanish DPA vs Banco Bilbao Vizcaya Argentaria, SA, 2020.

third-party analytical tools) were deposited on users' computers without prior consent.[68] Decisions also report[69] that when consent is withdrawn, unnecessary trackers are loaded. In certain cases,[70] non-essential cookies increased despite the user's attempts to reject them. Moreover, decisions refer to practices where cookies were stored after withdrawal of consent.[71] Such trackers encompassed statistics, social network cookies, and advertising cookies from third-party domains. Other practices relate to third-party cookies incorrectly categorised as technically essential, and consequently, when users unchecked the relevant boxes or clicked "reject all," non-essential cookies remained.[72] Such practices influence the users' freely given consent, which should be meaningful and unburdened by coercion, pressure, or dependence on non-necessary processing purposes. These online tracking practices can be attributed to the dark "forced action" pattern. Consent-based enforcement decisions seem to be riddled with design choices that are not easily noticeable and can have serious implications for users' control over their data. In this line, the European Commission plans to discuss with stakeholders how to improve consumer awareness of online tracking as part of its exercise to reach a "voluntary pledge to address the growing 'cookie fatigue' of internet users, namely the fact of having to continuously consent or refuse the processing of their data when landing on a website".[73]

Further concerns arise due to "design choices that fragment data protection information", making it difficult to access the necessary information required to make informed decisions. In particular, we found cases in which relevant information (e.g. on purposes, retention periods, etc.) was difficult to find and excessively spread out across several documents with buttons and links that must be activated to learn additional information.[74] Such practices contribute to the dark patterns of "obstruction" and "sneaking." While the GDPR mandates that data protection information should be easily accessible and provided in clear and plain language, the existence of dark patterns highlights the need for continued scrutiny and vigilance in ensuring users' control over their data.

Darkest dark patterns

Darkest patterns are detective design techniques purposely integrated into the system architecture (SA) or code level of an online service, and not on the UI. The system architecture constitutes the structural design of a digital product or application.[75] Making a determination of whether the darkest pattern has been used is challenging, and the regulatory case analysis did not render darkest dark patterns. Developers may use machine learning algorithms to analyse user behaviour and create personalised nudges or recommendations that steer users towards certain choices. These algorithms[76] may be designed to optimise for engagement or revenue rather than user well-being, leading to a system architecture that prioritises business goals over user needs.

---

[68] Luxembourg DPA vs Amazon, 2021; Belgian DPA vs Rossel & Cie, 2022; Belgian DPA vs Roularta Media Group, 2022; Danish DPA vs DMI, 2020; French DPA vs Microsoft, 2022; Spanish DPA vs Preicos Juridicos, 2021; Spanish DPA vs X commercial website, 2022; Spanish DPA vs Lia's Clothes, 2021; Spanish DPA vs Ramona Films S.L, 2022; Spanish DPA vs Iberia, 2020; Spanish DPA vs Marbella Resorts, 2021; Spanish DPA vs Radio Popular, 2021; Spanish DPA vs FDM, 2020; Spanish DPA vs Abanca Corporacion Bancaria, S.A., 2021; Spanish DPA vs Twitter, 2021; Danish DPA vs JAVA, 2020; French DPA vs Carrefour Group, 2020; Belgian DPA vs Y, 2019; French DPA vs Tiktok 2022; Italian DPA vs Uber Italy srl, 2022; Belgian DPA vs Y Housing Company, 2020.

[69] Belgian DPA vs Rossel & Cie, 2022.

[70] Belgian DPA VS Rossel Group, 2022.

[71] Belgian DPA vs Rossel & Cie, 2022; Polish DPA vs ClickQuickNow Sp. z o, 2019; French DPA vs Societe du Figaro, 2021; Spanish DPA vs FDM, 2020.

[72] Spanish DPA vs Vueling Airlines S.A., 2019

[73] EURACTIV.com, Luca Bertuzzi, 6th April, 2023, https://www.euractiv.com/section/data-privacy/news/cookie-fatigue-the-questions-facing-the-eu-commission-initiative/

[74] Irish DPA vs Whatsapp Ireland Limited, 2021; French vs Google LLC, 2019; Belgian DPA vs Rossel & Cie, 2022;Spanish DPA vs Twitter, 2021; Belgian DPA vs Telenet, 2021; Portuguese DPA vs INE, 2021; Spanish DPA vs Bodegas Dinastía, S.L., 2020; Belgian DPA vs Toerisme Vlaanderen, 2O22; Czech DPA vs Television operator, 2021; Danish DPA vs DBA, 2020;

[75] Stuart, A, 'System Architecture Design and Platform Development Strategies: An Introduction to Electronic Systems Development in the Age of AI, Agile Development, and Organisational Change' (1st edn, Oxford University Press 2022).

[76] UK Government. 'Algorithms: How They Can Reduce Competition and Harm Consumers' (Department for Business, Energy and Industrial Strategy, 2020) <https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers> accessed 29 March 2023.

Scholarship from algorithmic design classify these as deterministic algorithms.[77] An example of a "complex deterministic algorithm"[78] is a highly personalised recommendation that considers multiple factors, including user behavioural data and preferences. In complex deterministic design, a system gives the same output on similar inputs. In practice, an outside auditor could still inspect these kinds of algorithms embedded in darkest patterns and subject them to regulatory oversight. As a dark pattern is a deceptive design that manipulates users into doing something that they would not have done without either the manipulation or the design, a highly personalised recommender system achieves this design objective: the user acts upon a given recommendation that would not have been possible without the design.

On the other hand, "non-deterministic dark patterns"[79] are the most challenging to detect, audit and regulate. These patterns involve non-deterministic algorithms and/or machine learning systems or other opaque statistical methods that are difficult to understand.[80] The system is purposely designed to give different outputs to the same inputs. These patterns involve techniques such as "dark data collection"[81], "shadow profiling"[82], or data sharing practices that are not visible to users but impact their privacy or decision-making. These practices could also be considered the darkest patterns. Detecting non-deterministic patterns usually require insider information.

The use of opaque algorithms and machine learning techniques in darkest patterns poses a serious threat to user autonomy and control over personal data, and data subject rights[83], underscoring the importance of transparency and accountability in data processing practices. Despite their potential harm to users, few cases exist that shed light on such practice. One, however, involves Google's practice services of saving users' location data even after location tracking had been turned off in privacy settings. Despite users turning location data off, Google's architecture and code was programmed to automatically store time-stamped location data without asking.[84]

Algorithms can also amplify the impact of manipulative choice architecture.[85] For instance, if an algorithm decides which products are displayed to users based on factors such as popularity or profitability, this can reinforce the choice architecture by making certain options more visible or attractive. This can lead to a self-reinforcing cycle where the system architecture becomes increasingly optimised for the designer's goals rather than the user's. The Dutch Authority for Consumers and Markets (ACM) highlighted the risk of embedding algorithms to analyse consumer behaviour, preferences, and previous interactions in the system architecture to exploit the consumer

---

[77] GeeksforGeeks, 'Difference between Deterministic and Non-deterministic Algorithms' (GeeksforGeeks, no date) https://www.geeksforgeeks.org/difference-between-deterministic-and-non-deterministic-algorithms/ accessed 25 April 2023

[78] GeeksforGeeks, 'Difference between Deterministic and Non-deterministic Algorithms' (GeeksforGeeks, no date) https://www.geeksforgeeks.org/difference-between-deterministic-and-non-deterministic-algorithms/ accessed 25 April 2023

[79] Robert W Floyd, 'Nondeterministic Algorithms' (1967) 14(4) Journal of the ACM 636, https://doi.org/10.1145/321420.321422.

[80] Knuth, D. E. "Estimating the efficiency of backtrack programs," Math. Comput.29, 129 (Jan 1975), 121-136.

[81] Van Loon, R, 'Dark Data: What it is & How Businesses Should Address it' (2023) Simplilearn https://www.simplilearn.com/what-is-dark-data-article accessed 25 April 2023

[82] Aguiar, Luis, Christian Peukert, Maximilian Schäfer, and Hannes Ullrich. "Facebook shadow profiles." arXiv preprint arXiv:2202.04131 (2022); Moseley, T., Shye, A., Reddi, V. J., Grunwald, D., & Peri, R. (2007, March). Shadow profiling: Hiding instrumentation costs with parallelism. In International Symposium on Code Generation and Optimization (CGO'07) (pp. 198-208). IEEE.

[83] Sebastião Barros Vale and Gabriela Zanfir-Fortuna, Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities, FPF, 2022, https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf accessed 29 March 2023

[84] Google pays nearly $392 million to settle sweeping location-tracking case November 14, 2022https://www.npr.org/2022/11/14/1136521305/google-settlement-location-tracking-data-privacy#:~:text=Last%20month%2C%20Google%20settled%20a,advertisers%20with%20data%20on%20consumers.

[85] Psychology Today, 'AI Has Serious Implications for Choice Architecture' (5 October 2022) https://www.psychologytoday.com/us/blog/hovercraft-full-eels/202210/ai-has-serious-implications-choice-architecture accessed 25 April 2023; Karen Yeung, '"Hypernudge": Big Data as a mode of regulation by design' (2017) 20(1) Information, Communication & Society 118, DOI: <10.1080/1369118X.2016.1186713>; Simon Mills and Hans Sætra, 'The autonomous choice architect' (2022) AI & Soc, DOI: <10.1007/s00146-022-01486-z>; European Parliament, 'Understanding algorithmic decision-making: Opportunities and challenges' (2019) https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf accessed 25 April 2023.

decision-making process by manipulating the options presented to them.[86] For example, a designer may use an algorithm to recommend a more expensive product to the consumer by highlighting its features, while downplaying the features of a less expensive alternative. Furthermore, using "forced action" dark patterns may be automated through algorithms. A deceptive designer may use an algorithm to present a pop-up window with a call-to-action button that is hard to close or dismiss, forcing the consumer to take an unwanted action, such as signing up for a subscription.

Enforcement from a consumer law perspective

An examination of actions taken by the Consumer Protection and Cooperation (CPC) network and competition regulators shows that most cases of unfair and misleading commercial practices are linked to visible and darker dark pattern practices.

Visible dark patterns include obstructive refusal, urgency claims. Obstructive refusal practices are featured in decisions that made it difficult to refuse or unsubscribe a service[87] (e.g. refuse insurance). The Norwegian Consumer Council (NCC) and other European consumer organizations filed legal complaints against Amazon for creating obstacles for consumers to unsubscribe from its Prime service.[88] Other cases referred to the use of urgency messaging claims,[89] such as misleading countdown clocks in its online architecture to pressure consumers into making purchases. For example, following a coordinated Consumer Protection and Cooperation (CPC) network action, the two large online platforms, Booking.com and Expedia, improved the presentation of their accommodation offers, aligning them with EU consumer law.[90]

Darker dark patterns consist of forced practices, hidden costs, and lack of or hidden information, are less detectable and can result in consumer harm. Some "forced practices" that fall under the category of "forced action" have been reported in some decisions. These practices include binding consumers to premium subscriptions without their knowledge after a free trial period;[91] prompting users to register on a platform without disclosing that their data will be used for commercial purpose;[92] unclear auto-renewal policies that may result in users being charged for services they no longer use[93]. In certain decision-making contexts, consumers were faced with "hidden costs". Some decisions referred to the fact that certain subscriptions entailed charges,[94] or costs that were not clearly mentioned in the base price, and had optional extras often pre-selected,[95] and their presence only becomes evident after the purchase has been made, contributing to the dark pattern known as "sneak into basket". A "lack of adequate and essential information" was observed in other decision-making situations that was essential to make informed choices.[96] For example, in travel insurance policies that cover the risk of cancellation[97], or in websites that claim to provide price comparisons[98] but do not clearly display business names or disclose fixed charges to consumers[99]. In some instances, properties were marketed as "discounted" without revealing that the

---

[86] Autoriteit Consument en Markt (ACM), 'Guidelines on the Protection of the Online Consumer' (ACM, February 2020) https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf accessed 29 March 2023.

[87] AGCM vs Ryanair, 2013; CMA vs Microsoft's Xbox Live Gold and Game Pass products, 2022.

[88] Forbrukerrådet (Norwegian Consumer Council) press release, Amazon manipulates customers to stay subscribed (14 January 2021)., https://www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/

[89] CMA vs Emma Sleep group, 2022; CMA vs Viagogo, 2015. https://www.gov.uk/government/news/cma-investigates-online-selling-practices-based-on-urgency-claims

[90] European Commission press release, More transparency: Following EU action, Booking.com and Expedia align practices with EU consumer law (IP/20/2444, 18 December 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2444

[91] AGCM vs Edates, 2016.

[92] ICA vs Facebook, 2018.

[93] CMA vs Microsoft's Xbox Live Gold and Game Pass products, 2022.

[94] CMA vs Adaptive Affinity, 2011.

[95] ACM vs WTC, 2015; EU Commission vs Airbnb, 2019; CMA vs Viagogo, 2015.

[96] CMA vs Microsoft's Xbox Live Gold and Game Pass products, 2022.

[97] ICA vs Easyjet, 2013.

[98] CMA vs Heating oil price comparison websites - Fuelfighter.co.uk; Boilerjuice.co.uk; Cheapheatingoil, 2011.

[99] CMA vs Expedia, 2017.

price was based on a standard rate provided by the accommodation provider.[100] Such practices, which relate to the dark pattern of "hidden information" and “sneaking”, can undermine consumers' autonomy and decision-making, leading to adverse outcomes.

[100] CMA vs Expedia, 2017.

Table 1. Distribution of regulatory consumer and data protection cases according to the visibility spectrum and per dark pattern type

Domains	Visibility spectrum	Identified practices in regulatory decisions	Related dark patterns
Data protection cases	Visible	Pre-checked boxes	Preselection
		Bundling or tying practices	Forced Action
		Obstructive refusal or withdrawal options	Obstruction
		Wrong language	Language discontinuity
		Continuous nagging with commercial communications	Nagging
	Darker	Information that is complex and hard to understand	Obstruction
		Misleading practices	Misleading information and sneaking
		Forced practices	Forced Action
		Lack or hidden information	Hidden information (sometimes Sneaking)
	Darkest	--	--
Consumer law cases	Visible	Obstructive refusal	Obstruction
		Urgency claims	Urgency
	Darker	Forced practices	Forced registration
		Hidden costs	Sneaking (Hidden Costs)
	Darkest	--	--

Part II: Digital Design Across the Spectrum of Visibility

As highlighted in Part I, the prevalence of dark patterns and deceptive design practices in digital systems has become an increasingly pressing issue in the era of ubiquitous technology and the internet, as revealed by enforcement actions taken by regulators. Interestingly, current or evolving legislative initiatives of the EU do not attempt to directly regulate the role of designers or developers in the space of dark patterns but rather that of data controllers/businesses/platforms. Furthermore, the legislative focus has been on regulating the online graphical interface. However, it is becoming evident that most dark pattern practices are embedded in the underlying Code.[101] Accordingly, Part II of this article focuses on the mindset of developers and designers, as well as the role of regulatory oversight in controlling dark patterns and deceptive design practices built into the system architecture.

The Mental Model used by Designers and Developers

When designing complex online systems, designers and developers should not speak in terms of 'online interface' and 'system architecture'. For example, 'atomic' designers generally think of their user interfaces as a cohesive whole and a collection of modular parts operating simultaneously. The methodology of "atomic design"[102] is commonly used for creating systems and helps designers and developers create interfaces that are both consistent and scalable. However, atomic design breaks down user interfaces into smaller, more manageable components, making it easier for users to understand how to use a product or service. Using a modular approach, atomic design permits companies to easily add new features and functionality to their products and services. It achieves this by adopting metaphors from physics where groups of surface-level features (atoms) are viewed alongside other underlying protocols as "molecules" or groups of atoms, etc. In this respect, the "online interface" does not really exist, but features in this space are controlled and manipulated by the underlying "system". This difference in terminology challenges lawmakers who have a mental model of online interfaces and system architecture as independent of one another.

Designers, regardless of their position in management, product strategy, UX or research, are entrusted with creating the fundamental framework of digital services. However, design professionals aim to optimise user engagement, consent and client retention by employing suitable interfaces, text, juxtapositions and graphics that maximise revenues, despite the trade-offs involved with other parties. Achieving a balance between the needs of clients, businesses, and users is a challenging task that requires designers to reconcile individual beliefs with potential outcomes in practice. In certain cases, business interests may not align with user-centric designs, resulting in trade-offs that compromise users and other stakeholders. Due to time and budget constraints, designers may also face limited agency to improve the transparency and privacy-friendliness of digital artefacts. Consequently, prioritising business goals over user needs and desires may result in dark patterns that deceive or manipulate users. Gray et al. referred to such instances as "asshole designer"[103], where designers "explicitly assert control over the user's experience by implementing obnoxious, coercive or deceitful behaviours that primarily serve shareholders' interests".

Designers possess some general familiarity with ethics and best practices and awareness of methods or approaches that allow them to be more value-sensitive.[104] However, their knowledge of legal compliance with GDPR's data-protection-by-design and by-default obligations[105] and the fairness principles afforded by UCPD enforcement

---

[101] Jamie Luguri, Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, Journal of Legal Analysis, Volume 13, Issue 1, 2021, Pages 43–109, https://doi.org/10.1093/jla/laaa006

[102] Brad Frost, Atomic Design (Pittsburgh: Brad Frost Web, 2016).

[103] Colin M Gray, Shruthi Sai Chivukula, and Ahreum Lee, 'What Kind of Work Do "Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit' (2020) 2020 ACM Designing Interactive Systems Conference 61.

[104] Katie Shilton and Sara Anderson, 'Blended, not bossy: Ethics roles, responsibilities and expertise in design' (2016) 29 Interacting with Computers 71, DOI:https://doi.org/10.1093/iwc/iww002; Shaowen Bardzell, Jeffrey Bardzell, Jodi Forlizzi, John Zimmerman, and John Antanitis, 'Critical design and critical theory' (2012) Proceedings of the Designing Interactive Systems Conference on - DIS '12, 288 https://doi.org/10.1145/2317956.2318001.

[105] Article 25, Recital 78. GDPR.

actions is limited and may be viewed as only indirectly part of their core responsibilities.[106] Rather, the designer's role is to ensure that their design aligns with the software architecture and developer goals. The same lack of legal knowledge holds for developers. Online forums are an important source of legal information for software developers[107]; for example, the most common information that developers suggested on Stack Overflow related to GDPR legal compliance[108], in particular, developers frequently asked about how to adhere to privacy requirements that are imposed by various platforms, such as different app stores.[109] If the information given in such forums is not accurate or complete, this might render poor compliance practices with consequences to apps, programs and services that developers build. Moreover, developers are known to use code samples on the Web to build their applications, and tend to follow the default[110] options provided by large platforms (e.g. Google, Amazon, Apple). Some of these default options are graphical user interfaces with buttons and checkboxes, and others consist of code samples and such UI and codes are used without being informed about privacy consequences of their decisions on users.[111] Several UI[112] can lead to a higher data collection and user interfaces with dark patterns. Also, reused code samples can be deceptive code samples that developers merely copy-paste into their apps or programs without reading or knowing about what each line of the code does, and the consequences of such copy-pasting behaviour. Tahaei et al. show in their study that if developers copy and paste code samples from Google and Amazon mobile networks into their apps, they all lead to a dark pattern on the user side, e.g. presenting an UI without the possibility for users to reject consent to tracking, or using ambiguous textual statements (e.g. a code sample says “We may use your location” when Google uses the data for personalisation purposes).

The availability of advice from in-house legal teams with the appropriate knowledge to operationalise compliance principles into UI/UX user-centric design services may be necessary for designers and developers. Awareness and education of legal principles that impact users are essential to prevent deceptive UI/UX services. Providing practical guidance for practitioners can reduce uncertainty regarding legal requirements from a design and engineering perspective.

Their approach to developing digital systems should be ideally characterised by a value-centred[113] design that prioritises “human values”, intuitive and user-friendly experiences, and design decisions that benefit both users and stakeholders. In the dark patterns narrative, a shift towards a "design-driven organisation" is necessary[114], as

---

106 Mireille Hildebrandt, 'Algorithmic regulation and the rule of law' (2018) 376(2128) Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20170355.

107 Anton Barua, Stephen W Thomas, and Ahmed E Hassan. 2014. What are developers talking about? An analysis of topics and trends in Stack Overflow. Empirical Software Engineering 19, 3 (2014), 619–654.

108 Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding privacy-related questions on Stack Overflow. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–14.

109 Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. Proc. Priv. Enhancing Technol., 2 (2022), 114–131

110 Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. 2017. Stack Overflow considered harmful? The impact of copy&paste on Android application security. In 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 121–136; Mohammad Tahaei and Kami Vaniea. 2021. Code-Level Dark Patterns: Exploring Ad Networks’ Misleading Code Samples with Negative Consequences for Users. Position Paper at the “What Can CHI Do About Dark Patterns?” Workshop at CHI Conference on Human Factors in Computing Systems (CHI ’21), May 8–13, 2021, Yokohama, Japan; Abraham H. Mhaidli, Yixin Zou, and Florian Schaub. 2019. “We Can’t Live Without Them!” App Developers’ Adoption of Ad Networks and Their Considerations of Consumer Risks. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). 20.

111 Mohammad Tahaei and Kami Vaniea. 2021. “Developers Are Responsible”: What Ad Networks Tell Developers About Privacy. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21). Association for Computing Machinery, New York, NY, USA, Article 253, 1–11. https://doi.org/10.1145/3411763.3451805.

112 Santos, C., Nouwens, M., Toth, M., Bielova, N., Roca, V. (2021). Consent Management Platforms Under the GDPR: Processors and/or Controllers?. In: Gruschka, N., Antunes, L.F.C., Rannenberg, K., Drogkaris, P. (eds) Privacy Technologies and Policy. APF 2021. Lecture Notes in Computer Science(), vol 12703. Springer

113 Shruthi Sai Chivukula and Colin M Gray, 'Co-Evolving Towards Evil Design Outcomes: Mapping Problem and Solution Process Moves' (2020) Proceedings of DRS; Cockton, Gilbert. “Designing worth is worth designing.” Nordic Conference on Human-Computer Interaction (2006).

114 Shruthi Sai Chivukula, Chris Rhys Watkins, Rhea Manocha, Jingle Chen, and Colin M Gray. 2020. Dimensions of UX Practice that Shape Ethical Awareness. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–13.

user-centric design, and thus, deceptive design, is a multi-stakeholder issue. It requires shared responsibility between designers, developers/engineering teams, clients, the performance marketing team, legal teams, users, and the organisation's enforced values towards UX practitioners. Chivikula et al.[115] posit that "designers cannot solely ensure that the final product is ethically-mindful, but rather a shared responsibility across organisational functions". Therefore, designers must not overlook legal principles that permeate the kick-off, research, design, development, launch, and post-launch phases of a digital product or service and must not delegate accountability to other teams. Upholding this competence empowers designers and developers to discuss with other product/service chain stakeholders and avoid regulatory intervention. Ultimately, holding this knowledge enables designers and developers to balance the needs of the user with the needs of the business, ensuring that their products and services are optimised for both. This task can be challenging as designers and developers navigate a complex set of competing priorities and design constraints. However, it is crucial if designers and developers are to create digital systems that are user-friendly and effective.

Rethinking the Literal Definition of User Interface

The adoption of “interface” into the vernacular of regulators and law is fraught with challenges. Although this term appears extensively in the *digital design acquis* discussed in the next section, there is no scholarship on the appropriateness of the inclusion of this specific term. Janlert and Stolterman assert that the conventional definition of the "user interface" as a component of the physical surface of an interactive artefact or system is excessively restrictive.[116] The authors, returning to a literal interpretation of the interface as a surface, open fresh avenues for contemplating interactive technologies and faceless interactions (e. home assistants like Alexa, Google Home, Smart Speakers[117], and the multitude of “Internet of Things” devices on the market, etc).[118]

Two groups of modalities are identified by the authors: “*surface-bound”* and “*surface-free”*. Vision, touch, and direct object manipulations with hands and body that require a minimum targeted surface fall under “surface-bound” modalities. Some devices operate with “surface-free” modalities, using hearing, sound, smell, heat, wind, breath, balance, posture, and free gestures that do not necessitate touching. These modalities can be utilised in faceless interactions without requiring a target surface. The authors argue that the current dominant type of interaction is surface-bound, with the screen being the most preeminent surface.

Nevertheless, the risk of non-intuitive consequences in “surface-free” interactions are considerable. For instance, the authors note that “weak faceless interaction” can be achieved by replacing a keyboard with speech recognition, while “strong faceless interaction” entails solely of surface-free expressions and impressions. As “surface-free” modalities may add a layer of complexity, this carries implications for the design of digital systems and the user experience. Furthermore, the authors speculate on the likelihood of objects transforming into sentient, dynamic organisms when the entire surface of a digital device is coated with some touch-sensitive display paint, which could result in entirely new forms of interaction.

As we progress towards an era of increasingly intricate digital systems, designers and developers must consider the potential for novel forms of interaction where manipulative design practices occur beyond the traditional graphical user interface of digital systems. The concept of invisible and interfaceless interaction raises concerns about potential deceptive uses of surface-free interactions. The potential for surface-free or faceless interactions to be used in deceptive ways is significant. The hyper personalisation of voice assistants has already been deployed in the market.[119]

---

[115] Shruthi Sai Chivukula, Chris Rhys Watkins, Rhea Manocha, Jingle Chen, and Colin M Gray. 2020. Dimensions of UX Practice that Shape Ethical Awareness. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 1–13.

[116] Lars-Erik Janlert; Erik Stolterman, "9 Faceless Interaction," in *Things That Keep Us Busy: The Elements of Interaction* , MIT Press, 2017, pp.155-171.

[117] De Conca, Silvia, The Present Looks Nothing Like the Jetsons - Deceptive Design in Virtual Assistants and the Protection of the Rights of Users. Available at SSRN: https://ssrn.com/abstract=4412646 or http://dx.doi.org/10.2139/ssrn.4412646

[118] M Kowalczyk and others, 'Understanding Dark Patterns in Home IoT Devices' (2023) 179 CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems 1, https://doi.org/10.1145/3544548.3581432.

[119] 'AI Voice Bot: Drive Hyper-Personalization Across Different Industries' (NovelVox, 2023) https://www.novelvox.com/blog/ai-voice-bot-drive-hyper-personalization-across-different-industries/ accessed 27 April 2023

By challenging the conventional understanding of the interface as a mere surface and extending the metaphorical extension of "interface" to situations where little or no surface is provided, regulators can consider a deeper appreciation of the intricacy and richness of the interface concept: styles of interface thought, complexity and control, types of complexity, and faceless interaction all provide avenues for further and specific analyses. Hence, a redefinition of the interface concept that recognises the potential of surface-free and faceless interactions is required.

Therefore, adopting a holistic approach to design and regulation is crucial, considering the entire system architecture and the potential for surface-free or faceless interactions to be used in manipulative ways. This redefinition should inform the design practices of digital systems and the regulation of dark patterns and deceptive design techniques. Ultimately, this will lead to a better user experience and greater transparency in the design of digital systems. Such a transdisciplinary stance is posited by the recent guidelines from the EDPB[120] on deceptive design:

> "Qualitative and quantitative user research methods, such as A/B testing, eye tracking or user interviews, their results and their analysis can also be used to support demonstration of compliance." (EDPB)

Presently, the EDPB comprises only legal experts from DPAs[121], although it is noteworthy that the French[122] and UK Data Protection Authorities[123] each have one designer on staff. The EU Commission is assembling its enforcement team under the DSA, presenting an opportunity for designers and product managers to be recruited and provide their user experience and interface design expertise, thereby influencing the implementation of technology policy in software and systems.[124]

Systems of Manipulation

The previous section purposely adopts a broad definition of user interface. The *digital design acquis*, discussed in the following section, emphasises a meticulous focus on the user interface while overlooking the complex relationship between online interface, user experience (UX), and system architecture. The "online interface" is limited to the visual and interactive layer of a digital product or application with which users engage. It comprises layout, design, and aesthetic elements such as colours, fonts, and graphics. The interface prioritises usability, accessibility, and responsiveness to ensure a positive user experience.[125] The "User Experience" (UX) encompasses users' overall experience when interacting with a digital product or application. It includes usability, accessibility, performance, and user satisfaction.[126] UX is heavily influenced by the design of the online interface and the efficiency of the underlying system architecture. The "system architecture" constitutes the structural design of a digital product or application.[127]

---

[120] EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en accessed 15 March 2023

[121] EDPB, Who we are, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en

[122] Commission Nationale Informatique & Libertés, Shaping Choices in the Digital World, From dark patterns to data protection: the influence of ux/ui design on user empowerment, IP Report, Innovation and Foresight T N°06, https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

[123] The Information Commissioner's Office (ICO) promoted an event "Privacy, Seriously' organized by the in-house designer, gathering design, product leaders and legal scholars to discuss oh both law and design meet, availbale online at <https://ico.org.uk/about-the-ico/media-centre/events-and-webinars/privacy-seriously>; Privacy in the product design lifecycle, https://ico.org.uk/privacy-design

[124] Euroactiv, By Carline Sinders and Claire Pershan , 2022, available online at https://www.euractiv.com/section/digital/opinion/to-crack-down-on-dark-patterns-european-commission-needs-design-researchers/

[125] Jeff Johnson, Designing with the Mind in Mind: Simple Guide to Understanding User Interface Design Guidelines (3rd edn, Morgan Kaufmann 2020)

[126] Andreas Riener, User Experience Design in the Era of Automated Driving: 980 (Studies in Computational Intelligence 980, Springer 2021).

[127] Stuart, A, 'System Architecture Design and Platform Development Strategies: An Introduction to Electronic Systems Development in the Age of AI, Agile Development, and Organisational Change' (1st edn, Oxford University Press 2022).

However, this separate treatment is misguided and does not reflect modern design techniques. Boroji posits designers adopt an "iceberg model of design", made up of interconnected surface, skeleton, structure, scope, and strategy layers. For Boroji, the surface is just the tip of the iceberg.[128] By comprehending the interplay among these components, designers and developers can facilitate more nefarious patterns embedded deep in the system architecture.[129] As it typically encompasses the data flow, processing, storage, and communication between various components, a system would far more efficient at manipulating users through hypernudging at scale or engaging users with hyper-personalisation[130], if the entire architecture was designed for this end.

Designers must ensure that the interface design aligns with the technical requirements and constraints of the system architecture. Developers are accountable for implementing the online interface and guaranteeing its functioning within the system architecture. They must collaborate closely with designers to comprehend and translate the vision into a functional product. They must also ensure the system architecture supports the desired user experience and performance requirements. If the product is designed to stimulate user engagement, the patterns developers will integrate patterns into the system architecture that trigger outputs to stimulate and prompt users.[131]

Some dark patterns like nagging may be deployed and visibly malicious; others use psychological stimuli to trigger addiction-like behaviour.[132] System architectures utilising algorithms to curate content based on user preferences can create filter bubbles and echo chambers.[133] Sometimes these bubbles isolate users from diverse perspectives and reinforce their existing beliefs, to the benefit of the platform.[134] The darkest patterns embedded in the system architectures can exploit psychological bias like intermittent rewards and variable reinforcement schedules to encourage addictive behaviour and increase user engagement.[135] Common features like infinite scrolling, notifications, and gamification can manipulate users into spending more time on a platform or application than they otherwise would.[136] Addiction techniques like feedback loops can be implemented into the system architecture through various design and development strategies that exploit psychological principles and encourage addictive behaviour.[137] These techniques aim to increase user engagement, retain users, and maximise

---

[128] Hossein Boroji, 'The UX Iceberg Model: Understanding The User Experience' (Usability Geek, 6 June 2018) https://medium.com/usabilitygeek/ux-ice-berg-model-c1e31ec4d333 accessed 25 April 2023.

[129] For example of common design techniques, see Anuj Aggarwal, '10 Common Software Architectural Patterns in a Nutshell' (Towards Data Science, 2023) https://towardsdatascience.com/10-common-software-architectural-patterns-in-a-nutshell-a0b47a1e9013 accessed 25 April 2023.

[130] 'AI Voice bot: Drive Hyper-Personalization Across Different Industries' (NovelVox, 2023) https://www.novelvox.com/blog/ai-voice-bot-drive-hyper-personalization-across-different-industries/ accessed 25 April 2023

[131] B J Fogg, 'Persuasive technologies: Introduction' (n.d.) https://dl.acm.org/doi/fullHtml/10.1145/301353.301396 accessed 25 April 2023;B J Fogg, 'Mass interpersonal persuasion: An early view of a new phenomenon' in Harri Oinas-Kukkonen and others (eds), Persuasive Technology: Third International Conference, PERSUASIVE 2008, Oulu, Finland, June 4-6, 2008, Proceedings 3 (Springer Berlin Heidelberg 2008) 23-34; B J Fogg, 'Creating persuasive technologies: an eight-step design process' (2009) 4 Proceedings of the International Conference on Persuasive Technology 1-6;Ifeoma Adaji and Mosope Adisa, 'A Review of the Use of Persuasive Technologies to Influence Sustainable Behaviour' (2022) 30 Adjunct Proceedings of the ACM Conference on User Modeling, Adaptation and Personalization 317-325; Jiaming Wu and others, 'Sequential information design: Markov persuasion process and its efficient reinforcement learning' (2022) arXiv preprint arXiv:2202.10678 https://arxiv.org/abs/2202.10678 accessed 25 April 2023; Stefano Bassanelli and others, 'Gamification for behavior change: A scientometric review' (2022) 228 Acta Psychologica 103657.

[132] 'Addiction to Modern Technology: What the Science Says Free Collection of Articles Highlights the Latest Trends in Behavioral Addiction' (August 2017) https://www.journals.elsevier.com/addictive-behaviors-reports/news/addiction-to-modern-technology-what-the-science-says-free-co accessed 25 April 2023.

[133] Cass R Sunstein, Republic.com (Princeton University Press 2001); Cass R Sunstein, Republic.com 2.0 (Princeton University Press 2007).

[134] Pariser, E, The Filter Bubble: What the Internet Is Hiding from You (Penguin Press 2011).

[135] Manish Kumar and Anwesha Mondal, "A study on Internet addiction and its relation to psychopathology and self-esteem among college students", Industrial Psychiatry Journal 27(1) (2018), pp. 61-66.

[136] Woolley, K and Sharif, M A, 'The Psychology of Your Scrolling Addiction' (2022) https://hbr.org/2022/01/the-psychology-of-your-scrolling-addiction accessed 25 April 2023

[137] Dillard-Wright, D.B., 'Technology Designed for Addiction: What Are the Dangers of Digital Feedback Loops?' (2018) https://www.psychologytoday.com/us/blog/boundless/201801/technology-designed-addiction accessed 25 April 2023

the time they spend on a platform or application. Some standard addiction techniques that can be integrated into the system architecture.[138]

System architecture can be designed to exploit psychological principles that encourage addictive behavior and increase user engagement.[139] For instance, developers can implement features such as infinite scrolling, autoplay, and variable reinforcement schedules that manipulate users into spending more time on a platform than they otherwise would.[140] By providing users with unpredictable rewards or positive reinforcement at varying intervals, platforms can create a sense of anticipation and excitement.[141] To create these psychological stimuli, algorithms must be implemented in the system architecture that reward users sporadically or by introducing elements like virtual currency, badges, or points that can be earned and redeemed within the application. Rewards and different frequencies to keep users engaged require deceptive design in the system architecture; for example, social media platforms may use algorithms to show notifications and content at varying intervals, keeping users guessing when they'll receive the next "like" or comment.[142]

Developers can encourage continuous consumption of content by automatically loading new content as users reach the end of a page or a video. This can be implemented by using algorithms to fetch and display relevant content based on user preferences and behaviour. Integrating game-like elements such as challenges, leaderboards, and achievement systems into the architecture can enhance user engagement and motivation. System architecture that incorporates biased algorithms can have a negative impact on users. For example, a recommendation algorithm that prioritizes content based on factors such as popularity or engagement may inadvertently amplify controversial or harmful content, skewing users' perception of reality.

Part III: The new *digital design acquis* & the visibility spectrum

Organizations often use dark patterns to increase profits, gain a competitive advantage, or manipulate user behaviour. These practices are often driven by a larger economic system that prioritises short-term gains over long-term digital sustainability. This system rewards companies that engage in aggressive marketing and design tactics that prioritise shareholder value over the needs and preferences of users. To address this underlying issue, some scholars and activists have called for a broader shift towards a more ethical and sustainable economic system.[143] This would involve rethinking how businesses are structured and incentivised and creating new regulatory models that prioritise social impacts and a reduction of anti-competitive effects. This includes adopting new legal designed to promote competition and equity amongst market participants. This section scopes forthcoming legislation crafting dark pattern-specific laws and discusses its challenges from the perspective of the visibility spectrum. Herein we account the DSA, DMA, alongside the EU's proposals for new Data and AI Acts.

---

[138] Kimberly S Young, 'The Evolution of Internet Addiction' (2015) https://www.sciencedirect.com/science/article/pii/S0306460315001884 accessed 25 April 2023.

[139] Flayelle, M., Brevers, D., King, D.L. and others, 'A taxonomy of technology design features that promote potentially addictive online behaviours' (2023) 2 Nat Rev Psychol 136

[140] Collins, G., 'Why the Infinite Scroll is so Addictive' (10 December 2020) https://uxdesign.cc/why-the-infinite-scroll-is-so-addictive-9928367019c5 accessed 25 April 2023

[141] Jonathan Marciano, 'How Social Media Hacks Our Psychology' (Better Marketing, 15 September 2020) https://bettermarketing.pub/how-social-media-hacks-our-psychology-9f901f55e54a accessed 25 April 2023

[142] Barnhart, B, 'Everything You Need to Know about Social Media Algorithms' (Sprout Social, 26 March 2021) https://sproutsocial.com/insights/social-media-algorithms/ accessed 25 April 2023

[143] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford: Oxford University Press, 2019); Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019); Tim Wu, The Master Switch: The Rise and Fall of Information Empires (New York: Vintage Books, 2010); Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism (New York: PublicAffairs, 2013).

The Digital Services Act (DSA)

The DSA[144] is a legislative instrument regulating online intermediaries operating within the EU Single Market. This includes internet access providers, search engines, domain name registrars, hosting services, and online platforms, regardless of whether they are established in the EU or elsewhere. It has been designed to enhance user protection, increase transparency, and promote innovation.[145] Its wide scope of application demonstrates the commitment of the EU Commission - the new regulatory authority - to protect users across all online services and ensure that there is no legal loophole for the abuse of user rights. One of the key provisions of the DSA is Article 25, which prohibits the use of dark patterns in online interfaces. In this section, we will examine the scope of application of the DSA, the provisions regulating dark patterns, the decisional space it aims to protect, the covered practices, and how it tackles the visibility spectrum.

Article 25(1) DSA merely prohibits platforms[146] from designing, organizing, or operating their online interfaces[147] through different forms of influence "in a way that deceives or manipulates users or materially distorts or impairs their ability to make free and informed decisions". Unfortunately, Article 25 of the DSA is specifically applicable to "online platforms"[148] and does not extend to other entities that fall within the DSA's scope. Additionally, it does not encompass actors that frequently employ dark patterns but do not meet the criteria for 'online platforms' as defined in Article 2 of the DSA. The classification of on-platform games, such as Candy Crush, as 'online platforms' remains ambiguous.

Empirical studies[149] however report that dark patterns are a constant accorded the internet across websites and mobile apps.

The decisional space protected by the DSA refers to the ability of users to make autonomous and informed choices or decisions.[150] Recital 67 expands on this definition by including the autonomy of users and the impairment of their decision-making or choice. The user's decisional space is then defined as:

> *i) autonomy*[151] refers to the capacity to make one's own choices, by having the competency to do so and being able to authentically endorse the reasons for them,[152]

---

[144] 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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014

[145] European Commission, 'Digital Services Act Package' (Digital Strategy) https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package accessed 15 March 2023

[146] According to the regulation, online platform means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of the regulation.

[147] 'Online interface' means any software, including a website or a part thereof, and applications, including mobile applications (Article 3 (m) of the DSA).

[148] Article 3(m), DSA.

[149] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Mobile and Web Modalities. Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 377 (October 2021), 29 pages. https://doi.org/10.1145/3479521; Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In Proc. of CHI; Arunesh Mathur, Gunes Acar, Michael Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proc. ACM Hum.-Comput. Interact. 1, CSCW (2019).

[150] Recital 45 acknowledges the importance of providing information and transparency to users, which ultimately empowers them to make informed choices.

[151] Personal autonomy, as defined by Susser et al., refers to one who has the competencies (cognitive and affective) to consider one's choices and to act upon them,Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. Internet Policy Review, 8(2), 1–22. https://doi.org/10.14763/2019.2.1410

[152] Article 24 deals with transparency measures for online interfaces, which are crucial for user autonomy and informed decisions. It requires providers of intermediary services to disclose any direct or indirect remuneration, economic incentives, or other conditions that might influence the ranking of content. This disclosure enables users to understand the factors influencing the content they see and make informed decisions; Autonomy is also a central theme of the DSA - See Article 14

ii) choice is the user's options[153], and

iii) decision implies actions or behaviours that manifestation former choices and which are externally manifested and visible.[154]

Recital 67 of the DSA provides additional context and clarification on the prohibition of dark patterns of Article 25. The language used in this provision might not be familiar to digital designers, but it is important to understand what is meant by "structure, design, or functionalities" in the context of the DSA. In this context,

i) "*structure*" refers to the overall layout and organization of an online interface or a part thereof,

ii) "*design*" refers to the visual elements of an online interface, such as color schemes, typography, and imagery,

iii) "*functionalities*" refers to the technical features of an online interface, such as the way buttons, forms, and interactive elements function or work.

The DSA aims to protect users' autonomous decisions and choices by prohibiting various types of practices. It includes those that manipulate[155], deceive, materially distort, materially impair, nudge**,** and exploit user's choices, decision making and autonomy. There are two ways one can interpret this provision. *First,* the prohibition on the use of these different influence types is not clarified; accordingly, the undefined and unbound space surrounding these influence-types might trigger legal uncertainty, lack specificity and lead to different interpretations for designers, developers, regulators, policy-makers to foreground and disambiguate, each according to its own pursuits. *Second,* the broad and abstract sense of this catch-all provision might, on the other hand, be read as an anticipatory provision for future-proofing emerging technologies and new influence-types that impacts a user's behaviour. The latter perspective will be influenced by the scope assigned to the DSA, specifically whether it is limited to the user interface or extends beyond it.

Article 25(2) provides an *exception* that exempts "practices already covered" by Directive 2005/29/EC or Regulation (EU) 2016/679, implying that these practices might be prohibited by existing legislation which include the UCPD and GDPR. This exception raises concerns about the effectiveness of the provision in combating dark patterns as almost all identified dark patterns fall under the scope of both the GDPR and UCPD[156]. As a result, dark patterns practices involving personal data are covered by the GDPR, and all dark patterns involved in B2C transactions are covered by the UCPD. However, due to the subsidiary nature of the DSA, certain dark patterns might not be covered by existing legislations, such as infinite scroll, auto play, nagging practices. These practices might also include business-to-business activities that are not governed by the UCPD. Additionally, it is unclear whether the DSA covers darker and darkest dark patterns, such as video, pop-ups, vocal interaction, virtual assistants, call, and chatbots. The wording adopted in Article 25(1), "design, organize, or operate" seems to scope the *classical graphical user interface (GUI*). However, it seems to sidestep the next-generation dark patterns that are not currently caught by existing legislation, such as personalized hypernudges, human-robot manipulation, voice and haptic interfaces, and augmented and virtual reality. "Dark patterns in the metaverse" might require additional regulation. While Recital 67 mentions presenting choices in a non-neutral manner, it is not clear what a "neutral manner" means. This lack of clarity might lead to different interpretations of what constitutes a dark pattern, which could result in legal uncertainty and make it difficult to enforce the provisions of the DSA.

Furthermore, Article 25(3) grants the Commission the power to issue guidelines on how the prohibition in paragraph 1 applies to specific practices. This provision highlights the possibility of forthcoming regulations that would further clarify the prohibition of dark patterns in online interfaces.

(Content Interference via Terms and Conditions), Article 20 (Complaint Handling), Article 38 (Recommender Systems), Article 25 (Dark Patterns).

153 Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. Internet Policy Review, 8(2), 1–22. https://doi.org/10.14763/2019.2.1410

154 Articles 14, 24, & 25, DSA.

155 Manipulation has not been defined yet in EU law and requires further elaboration and disambiguation regarding other influence types.

156 OECD, "Dark commercial patterns" (2022) OECD Digital Economy Papers, No. 336 at 31 and Annex F..

The DSA also introduces *new obligations* and responsibilities for online platforms. One of these is to conduct regular risk assessments and implement risk mitigation measures to prevent or limit the negative effects of their services on public interests, such as democracy, public health or security.[157] These measures include transparency, oversight, accountability and user empowerment mechanisms.[158] Risk mitigation measures are applicable to all online platforms that provide services within the EU, regardless of their size or origin. However, VLOPs have to comply with more stringent obligations on risk assessments, risk mitigation measures and independent audits than smaller and emerging platforms.[159] Regulators may fit in dark patterns-based risk mitigation measures by enforcing laws and guidelines that protect consumers from unfair and deceptive practices online.[160] Some of these measures may include:

- Requiring clear and conspicuous disclosure of material information
- Prohibiting misleading or coercive tactics that influence user behavior
- Ensuring users have meaningful choice and control over their data and preferences
- Providing users with easy ways to opt out or cancel services
- Monitoring and auditing compliance with privacy and consumer protection laws

The regulator would focus on the outcomes and impacts of dark patterns, rather than the specific design techniques used by service providers. This way, the regulator can address a broader range of issues and challenges that may arise. By following these measures, regulators can help prevent or limit the negative effects of deceptive design on public interests. This approach may help protect consumers from being misled or coerced by dark patterns, and encourage service providers to be more transparent and ethical in their design choices. On the other hand, it may also face some difficulties defining and identifying, enforcing compliance, and balancing innovation with regulation. Therefore, a pluralistic approach that combines different regulatory regimes and strategies may be more effective.[161]

Recital 83 also refers to *risks* stemming from the "design, functioning or use, including through manipulation, of very large online platforms and of very large online search engines with an actual or foreseeable negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence. Such risks may also stem from coordinated disinformation campaigns related to public health, or from online interface design that may stimulate behavioural addictions of recipients of the service". While the language in the DSA does not explicitly mention dark patterns that exist below the surface in the system architecture, such as the use of algorithms or data practices, it is posited that these practices could be considered as part of the "functionalities" of an online interface or a part thereof. This would require creative judicial interpretation in the language of the Act.

When risk is unknown, or its impact uncertain, one possible regulatory strategy is for policy makers, organisations, and other stakeholders to adopt the precautionary principle, especially when the science around the risk is unknown or the impact indeterminable.[162] The DSA is an example of risk regulation.[163] Article 35, DSA outlines various risk mitigation measures that VLOPs and very large online search engines must implement to address systemic risks; two of which are related to deceptive design. First, Article 35 (1)(a) states platforms can me

[157] Article 34, Digital Services Act

[158] Article 34 (2), Digital Services Act

[159] Article 34, Digital Services Act; Note Article 35 mandates VLOPs undertake risk mitigation measures based on outcomes from the Risk Assessment. Recital 90 elaborates on the need for VLOPs to adopt measures that prevent or mitigate the risks identified in their assessments, in order to protect the public interest; Article 37 - External audit: This article requires VLOPs to submit their risk assessments and information on the adopted risk mitigation measures to an independent external auditor for review.

[160] Article 34(1)(a), Digital Services Act

[161] Mark R Leiser, 'Dark Patterns: The Case for Regulatory Pluralism between the European Union's Consumer and Data Protection Regimes' in Research Handbook on EU Data Protection Law (Edward Elgar Publishing 2022) 240.

[162] Derczynski, L., Kirk, H. R., Balachandran, V., Kumar, S., Tsvetkov, Y., Leiser, M. R., & Mohammad, S. (2023). Assessing Language Model Deployment with Risk Cards. arXiv preprint arXiv:2303.18190.

[163] Robert Baldwin, Martin Cave, and Martin Lodge. 2012. Understanding Regulation: Theory, Strategy, and Practice (2nd ed ed.). Oxford University Press, New York

directed to mitigate the risk from deceptive design by “adapting their services' design, features, or functioning, including online interfaces”. Second, platforms my be asked to take “awareness-raising measures and adapting their online interface”.

The Digital Markets Act

The Digital Markets Act[164] (DMA), introduced by the European Commission, aims to address the role and unfair practices of certain online platforms that qualify as "gatekeepers"[165]. The DMA identifies quantitative parameters to determine whether a large online platform is a "gatekeeper" based on its impact on the internal market, the provision of a core platform service connecting a large user base to many businesses, and an entrenched and durable market position.[166] By identifying gatekeepers in this way, the DMA enables regulators to focus on platforms that are most likely to engage in dark patterns and other unfair practices. Gatekeepers provide platform services that include online intermediation, search engines, social networks, video-sharing, number-independent interpersonal communication services, operating systems, cloud computing services, advertising, and more.[167]

The DMA also introduces provisions related to dark patterns, emphasising that gatekeepers must not engage in behaviour that undermines the effectiveness of the prohibitions and obligations laid down in the regulation.[168] This includes using non-neutral design, presentation of end-user choices, or subversion of user autonomy, decision-making, or choice through the structure, function, or operation of a user interface or part thereof. The language used in the DMA provisions echoes the proposed Deceptive Experiences to Online User Reduction (DETOUR) Act in the US[169], which defines dark patterns as subverting end-users' autonomy, decision-making, or free choice.[170] This definition has been adopted in the California Privacy Rights Act (CPRA)[171] and the new Colorado Privacy Act.[172] The DMA also introduces a range of provisions designed to prevent gatekeepers from engaging in dark patterns. For example, Recital 70 of the DMA emphasises the importance of applying rules to any practice by a gatekeeper, regardless of its form, insofar as it corresponds to the type of practice that is the subject of one of the obligations laid down by the Act. This includes the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using the structure, function, or manner of operation of a user interface or a part thereof to subvert or impair user autonomy, decision-making, or choice.

In this context, gatekeepers should not rely on dark patterns which can subvert and impair user autonomy, decision-making, and choice when designing their digital interfaces.[173] However, the provisions are unclear on whether the term “user interface” strictly refers to the interface design of a company or includes the user experience and language used. The example of a time-consuming and cumbersome decision highlights the importance of enabling users to unsubscribe from a core platform service with ease.

Article 13(6) of the DMA prohibits gatekeepers from degrading the conditions or quality of any core platform services provided to business users or end users who avail themselves of the rights or choices laid down in Articles 5, 6, and 7. This includes offering choices to the end-user in a non-neutral manner or subverting end-users' or business users' autonomy, decision-making, or free choice via the structure, design, function, or manner of operation of a user interface, or a part thereof. These provisions align with the definition of dark patterns as manipulative design techniques that push or deceive users into decisions that have negative consequences for them, which is important for protecting user rights and ensuring fair competition in the online market.

---

164 Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

165 Article 2(1), Article 3, Recital 16, Digital Markets Act

166 European Commission, 'Digital Markets Act: Ensuring Fair and Open Digital Markets' (European Commission) https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en accessed 15 March 2023

167 Article 2(2), Digital Markets Act

168 Article 13(6)

169 Deceptive Experiences To Online Users Reduction Act or the DETOUR Act, H.R.6083, 117th Cong. (2021-2022).

170 Section 3(a)(1), DETOUR Act

171 California Privacy Rights Act (CPRA) https://cpra.gtlaw.com/cpra-full-text/

172 SB21-190 Protect Personal Data Privacy https://leg.colorado.gov/bills/sb21-190

173 Recital 70, Digital Markets Act

Additionally, Article 5 of the DMA requires gatekeepers to provide business users access to data generated through their transactions with end-users on the platform unless the data is subject to intellectual property or data protection rights:

> "refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end-users to other services … to combine personal data, unless the end-user has been presented with the specific choice and provide consent in the sense of Reg.2016/679 (i.e., the GDPR) …"

Article 5(f) also contains a prohibition to require "business and end users to subscribe to or register with any other core platform services …" offered by the gatekeeper, thereby obviously limiting the amount of personal data that gatekeepers can accumulate. This provision aims to increase transparency and foster competition, allowing businesses access to valuable data that can inform their strategies and decision-making processes. However, according to Article 6 of the DMA, gatekeepers are not allowed to leverage their access to this data in a discriminatory manner. This provision prohibits gatekeepers from using data to unfairly compete with other businesses or impede access to the platform. Moreover, gatekeepers must provide business users with clear and transparent information on how their data is collected, processed, and used, as well as on the platform's access and use conditions. Furthermore, Recital 69 of the DMA acknowledges the importance of user trust and the negative impact that dark patterns can have on user autonomy and decision-making. In line with this definition, Recital 70 clarifies that gatekeepers must not engage in any behaviour that would undermine the effectiveness of the prohibitions and obligations laid down in the DMA, including the use of non-neutral user interface design or the subversion of user autonomy, decision-making, or choice.

The Data Act Proposal

The Data Act[174] would apply to data sharing and data portability activities. It does not override or contradict the GDPR[175], but rather builds on the Regulation and provides more specific guidance for data sharing and portability. Ultimately, the Data Act will set out the conditions and requirements for facilitating data flows among different actors.[176] The EU believes that having two different regulations is necessary to address the challenges and opportunities of the digital economy and society. Accordingly the Data Act proposal aims to foster innovation, competition and the public interest by enabling more data access and reuse among different actors. While the GDP aims to protect users' privacy, dignity and autonomy by ensuring their data is processed lawfully, fairly and transparently; in theory, the Data Act will facilitate greater access to and use of data, allowing users to access and port to third parties the data generated through their use of connected products and services.

The Data Act does not introduce a new definition or test for dark patterns but rather refers to the existing concepts and criteria from the GDPR and other regulations. However, it is possible that some practices that are not considered dark patterns under the GDPR could be considered dark patterns under the Data Act. This could happen if these practices interfere with users' rights or choices regarding data sharing or portability. For example, a website that does not ask for consent to process personal data may not violate the GDPR if it has another legal basis for doing so. But if this website makes it hard for users to access or transfer their data to another service provider, it could violate the Data Act. A website that offers incentives or rewards for users who agree to share or process their data in ways that are not necessary for the service should amount to a dark pattern.

The Data Act aims to cover a wider range of dark patterns that may hinder users from exercising their rights under data protection law, such as data access, data portability or data erasure.[177] An example of such a dark pattern could be a website that makes it difficult for users to delete their accounts or transfer their data to another service provider by hiding these options in complex menus or requiring multiple steps to complete these actions.[178]

---

[174] Regulation on harmonised rules on fair access to and use of data (Data Act)

[175]

[176] European Commission, 'Commission proposes new measures to protect EU businesses from unfair trading practices', Press release IP/22/1113 (Brussels, 6 April 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 accessed 19 April 2023.

[177] Article 6(2)(a), Data Act (Proposal) from the EU Council's version.

[178] Recital 34, Data Act (Proposal).

Another example could be a website that uses emotional language or social pressure to discourage users from opting out of data sharing or processing activities.[179] However, it is possible that some practices that are not considered dark patterns under the GDPR could be considered dark patterns under the Data Act. This could happen if these practices interfere with users' rights or choices regarding data sharing or portability. For example, a website that does not ask for consent to process personal data may not violate the GDPR if it has another legal basis for doing so; however, if a dark pattern makes it hard for users to access or transfer their data to another service provider, it could violate the Data Act.

Any third party that receives data is obligated not to "coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user". Recital 34 explains that this means that third parties should not rely on dark patterns when designing their digital interfaces, particularly in a way that manipulates consumers to disclose more data — the third party should therefore comply with the data minimisation principle as defined in the GDPR to ensure that they do not employ dark pattern practices in their interfaces.

AI Act Proposal

The AI Act proposal[180] sets out rules on the development, placement on the market, and use of artificial intelligence systems ("AI systems") across the EU.

Article 3 point 1 of the proposal defines an AI system. It refers to i) a software that is developed with one or more of the techniques and approaches listed in Annex I, which include, for example, machine learning (ML), statistical and knowledge representation approaches; and ii) can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. For example, if a given AI system deploys ML and generates UI-based content, or recommendations at UI-level, then such a system will be covered by the AI act. In this scenario, the AI act has the potential to cover darkest dark patterns.

Although this proposal is still undergoing the legislative process, it prohibits manufacturers of AI systems from placing on the market, put into a service, or use dark patterns within AI systems. This groundbreaking legislation prohibits manufacturers from incorporating dark patterns into their AI systems. Article 5(1)(a) and (b) of the proposal details two critical provisions:[181]

(a) AI systems must not employ subliminal techniques that manipulate behaviour, causing physical or psychological harm.
(b) AI systems must not exploit the vulnerabilities of specific groups, such as age, disability, or socio-economic status, to manipulate behaviour and cause harm.

Article 5(1)(a) refers to subliminal techniques regarding sensory stimuli which are below the threshold for conscious perception. Franklin et al.[182] claims that the psychological research community has not drawn a firm consensus about the efficacy of subliminal techniques. Trappey et al.[183], in their meta-analysis of the effectiveness of subliminal stimuli, found that it had a low effect size which was not statistically significant.

[179] "The characteristics of the AI system, such as their opaque nature or their complexity, can make it difficult to understand their decision-making processes, which can lead to the adoption of the AI system without knowing its impact and limitations."

[180] European Council, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' (2022) ST 14954, https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf accessed 27 April 2023.

[181] Veale, M.; and Borgesius, F. Z. 2021. Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International , 22(4): 97–112.

[182] Franklin, M., Ashton, H., Gorman, R., & Armstrong, S. (2022). Missing Mechanisms of Manipulation in the EU AI Act. *The International FLAIRS Conference Proceedings*, *35*. https://doi.org/10.32473/flairs.v35i.130723.

[183] Trappey, R. J.; and Woodside, A. 2004.bBrand choice: revealing customers' unconscious-automatic and strategic thinking processes. Springer.

Accordingly, several authors[184] suggest that subliminal techniques should be replaced with a broader range of manipulation techniques.

Concerning the harms caused by manipulative AI systems, only physical or psychological harms are mentioned in the proposal. However, important harms need to be considered, such as societal harms "harming the democratic process, eroding the rule of law, or exacerbating inequality",[185] time, addiction and autonomy.[186]

Article 5(1)(b) of the AI Act prohibits AI practices involving systems that exploit and target the vulnerabilities of specific groups of individuals, such as age, disability, or socio-economic status, to manipulate behaviour. However, this provision only regards "specific groups". It is important to consider that not only specific groups but that *all* human beings become vulnerable when their unique weaknesses are exploited.[187]

AI-based dark patterns can consist of sophisticated, dynamic practices that employ real-time adjustments to a website/online service's user interface or user experience. Moreover, AI-based dark patterns can also have the potential of being optimized[188] to induce specific online behavior (micro-targeted dark patterns).

Powered by machine-learning algorithms, and leveraging user data inputs and "personalized persuasion profiles"[189] companies can create personalized dark patterns with remarkable precision over time. Such data inputs can consist of fine grained targeting that range from IP addresses, demographics (age, gender), matching demographic characteristics with observed behaviour, psychographic targeting data that rely on psychological insights into the personality styles and behaviour of a consumer.[190] With these and many other heterogeneous data points, algorithmic-based dark patterns are then able to cyclically adapt to their users by learning about them and building on individual biases, preferences and needs and that can be purposefully be manipulated[191] through customised choice interfaces (affecting the user's ability to rationally deal with a particular choice). Helberger et al. posit that "By constantly learning more about one's consumers' characteristics and their responses to particular cues, the potential for effective manipulation also grows". For instance, a shopping website might customize the design of a checkout page for User A to boost sales, while presenting different options, pricing, notifications, and offers to User B. Individualizing user's choices puts the platform/website/app in control of what each person is allowed to know and act accordingly (privacy choices, purchases, etc), i.e., in a "factual position of ownership of the information economy"[192], emphasising even more the power imbalances between users and traders. This adaptability and algorithmic customization trend underscores the growing concern surrounding the impact of dark patterns on consumer decision-making and highlights the need for robust enforcement and oversight to avoid weaponizing these types of dark patterns against users.

Although no substantial evidence currently indicates the widespread use of personalized dark patterns targeting individual vulnerabilities, the growing convergence of data collection, machine learning, and AI techniques may alter this landscape.[193] In this line, the OECD anticipate that businesses will increasingly tailor dark patterns,

---

[184] Uuk, R. 2022. UManipulation and the AI Act. The Future of Life Institute;Franklin, M., Ashton, H., Gorman, R., & Armstrong, S. (2022). Missing Mechanisms of Manipulation in the EU AI Act. *The International FLAIRS Conference Proceedings*, *35*. https://doi.org/10.32473/flairs.v35i.130723; https://oecd.ai/en/wonk/ai-act-manipulation-methods accessed 24 April 2023.

[185] Uuk, R. 2022. UManipulation and the AI Act. The Future of Life Institute.

[186] Franklin, M., Ashton, H., Gorman, R., & Armstrong, S. (2022). Missing Mechanisms of Manipulation in the EU AI Act. *The International FLAIRS Conference Proceedings*, *35*. https://doi.org/10.32473/flairs.v35i.130723.

[187] Helberger, N. et al. (2021), EU consumer protection 2.0 Structural asymmetries in digital consumer markets; Franklin, M., Ashton, H., Gorman, R., & Armstrong, S. (2022). Missing Mechanisms of Manipulation in the EU AI Act. *The International FLAIRS Conference Proceedings*, *35*. https://doi.org/10.32473/flairs.v35i.130723.

[188] Congressional Research Service, 'What Hides in the Shadows: Deceptive Design of Dark Patterns'(2022) <https://sgp.fas.org/crs/misc/IF12246.pdf> accessed 27 March 2023, pp. 2

[189] Helberger, N. et al. (2021), EU consumer protection 2.0 Structural asymmetries in digital consumer markets.

[190] Helberger, N. et al. (2021), EU consumer protection 2.0 Structural asymmetries in digital consumer markets.

[191] Susser, Daniel, Beate Roessler, and Helen Nissenbaum. 2019. 'Technology, Autonomy, and Manipulation.' Internet Policy Review 8 (2). https://doi.org/10.14763/2019.2.1410.

[192] Helberger, N. et al. (2021), EU consumer protection 2.0 Structural asymmetries in digital consumer markets.

[193] OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en; Mills, S. (2022). Personalized nudging. Behavioural Public Policy, 6(1), 150-159. doi:10.1017/bpp.2020.7

enabling them to target consumers' vulnerabilities with a high level of granularity, [194] and trigger collective harms in mass. The European Commission (EC) recognizes the existing evidence gap on the impact of personalized dark patterns on user decision-making and suggests that, despite ethical challenges, future research needs to investigate alternative personalization methods that employ similar personality traits without resorting to invasive data collection or exploiting vulnerabilities.[195]

Algorithmic-dark patterns can be more difficult to detect and measure rather than known transactional dark patterns[196] because differences between each individual make it more difficult to distinguish targeted vulnerabilities from other benign or tolerable persuasive practices. Detection and measurement methods (e.g. multiple crawlers in a large-scale analysis using different settings and across modalities) are needed to discern the possible proof and causal link of a situated personalised dark pattern appearing to a concrete person whose behavior got manipulated. It is also challenging to reliably state that any observed differences are due to personalization, rather than to A/B testing, dynamism, time, randomness, etc..

Article 9 of the AI Act mandates a risk assessment for AI systems, including the identification and analysis of known and foreseeable risks to health, safety, and fundamental rights associated with high-risk AI systems. As this provision encompasses both consumer protection and privacy fundamental rights, it can be interpreted more broadly[197] to address algorithmically-driven dark patterns and algorithmic system designs that cause behavioral harms, such as addiction and loss of control.

The proposed AI Act emphasises the importance of designing and developing AI systems that comply with applicable law and ethical principles, safeguard safety throughout their life cycle, and ensure that the results are accurate, robust, and reliable. A transdisciplinary approach involving collaboration between designers, developers, and regulators is crucial to achieving this. Qualitative and quantitative user research methods such as A/B testing, eye tracking, or user interviews can support the demonstration of compliance with regulations.

> "To ensure that AI systems operate in a manner that complies with applicable law and ethical principles, the designers and developers of AI systems should ensure that they use a holistic risk management approach throughout the AI system's life cycle." (Proposed AI Act)

With Meta already testing AI in consumer marketing[198], and ChatGPT-4 envisaged as deployed as a medium between platforms and consumers, traditional means of delivering terms and conditions, privacy policies, and other transparency obligations will be powered by new forms of machine-learning holding the potential for further and surreptitious manipulative practices.[199]

Synthesis

The EU established a regulatory patchwork applicable to dark patterns with different types of protection and harms. Both data protection and consumer laws include *generally-phrased obligations* that are applicable to dark patterns. Data protection law triggers legal protection against dark patterns through overarching principles (fairness, transparency, data protection of data by default and by design, etc) and consent legal requirements that are not specific to dark patterns and regard *individual harms* of affected data subjects. Consumer law, in particular the UCPD, prohibits certain types of professional practices that would lead consumers to take a decision that they

[194] OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

[195] EC (2022), Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. Final Report.

[196] Strahilevitz, Lior, Cranor Lorrie Faith, Marotta-Wurgler Florencia, Mayer Jonathan, Ohm Paul, Strandburg Katherine, Ur Blase, Benthall Sebastian, Lancieri Filippo Maria, Luguri Jamie & Verstraete Mark. 2019. Subcommittee Report: Privacy and Data Protection, Stigler Center Committee for the Study of Digital Platforms (2019).

[197] Jennifer King, 'Do the DSA and DMA Have What It Takes to Take on Dark Patterns?' (Tech Policy Press, (23 June, 2022) https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/ accessed 15 March 2023.

[198] The Drum, 'Production, Analytics, Measurement: Meta and Marketers Mull AI's Use Cases' (28 February 2023) https://www.thedrum.com/news/2023/02/28/production-analytics-measurement-meta-and-marketers-mull-ais-use-cases?utm_campaign=newsletter_daily_europe_pm&utm_source=pardot&utm_medium=email accessed 15 March 2023.

[199] New York Post, ChatGPT update tricks human into helping it bypass CAPTCHA security test; https://nypost.com/2023/03/17/the-manipulative-way-chatgpt-gamed-the-captcha-test/, accessed 4th April 2023.

otherwise would not have taken. Conversely, the DSA, DMA, and Data Act proposal provide for *dark patterns-specific provisions*, defining in concrete the concept of dark patterns and containing requirements on how to design interfaces. Regarding harms, both types of consumer and data protection regimes seem to focus on *individual harms* that can be caused by dark patterns. In contrast, the DSA and DMA regard *collective harms*. The DSA, due to the fact it is addressed to very large platforms and search engines, and the DMA, scoping gatekeepers, goes beyond individual harms and encompass instead a collective dimension of harms (or other legal consequences that can be triggered by dark patterns). The AI act proposal instead scopes in its provisions merely *for individual harms* (physical or psychological harm). Table 2 provides an overview of the regulatory framework applicable to dark patterns with different types of the scope of protection.

Digital Design Acquis	Types of provisions	Harms	Coverage	Authors' analysis
GDPR	generally-phrased obligations	individual	UI/UX	UI/UX
UCPD	generally-phrased obligations	individual	UI/UX	UI/UX
DSA	dark patterns-specific (platforms)	collective	UI/UX	UI/UX/SA
DMA	dark patterns-specific (gatekeepers)	collective	UI/UX	UI/UX/SA
Data Act proposal	dark patterns-specific	collective	UI/UX	UI/UX/SA
AI Act Proposal	dark patterns-specific	individual	Potentially SA	Potentially SA

Table 2. Regulatory framework applicable to dark patterns with different types of provisions, harms covered, enforcement levels and dark patterns covered within the visibility spectrum.

Table 3 provides an overview of the digital design acquis per legal instrument.

Legal Framework	Scope of Application		
	Article	**Recital**	**Exclusions**
Digital Services Act	**25**: prohibits design, organise or operate their **online interfaces** in a way that deceives or manipulates users or materially distorts or impairs their ability to make free and informed decisions"	**67:** "structure", "design" "Functionalities" of the UI	Practices covered by the GDPR and/or UCPD
Digital Markets Act	**13 (6)**: by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a **user interface**	**37:** structure, design, function or manner of operation	Non-Gatekeepers
Data Act (proposal)	**6(2)(a):** "coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital **interface** with the user"	**34:** manipulative techniques can be used to persuade users, particularly vulnerable consumers, to engage in unwanted behaviours, and to deceive users by nudging them into decision on data disclosure	Non-data sharing & portability practices

AI Act (proposal)	**A5(1)(a)(b)**: prohibits AI systems that - employ subliminal techniques that manipulate behaviour; - exploit the vulnerabilities of specific groups, to manipulate behaviour and cause harm	**R16:** intention to materially distort the behaviour of a person and in a manner that causes or is likely to cause (e.g., psychological) harm to that or another person	Non-AI enabled systems (e.g., no ML techniques)

Table 3 Scope of application of the DSA, DMA, Data Act and AI Act proposals to dark patterns and their exclusions.

Part IV Conclusion and Recommendations

This article examined the current state of enforcement decisions regarding dark patterns and the challenges of implementing laws to address them. Based on our analysis of legal cases pertaining to consumer law and data protection, we found that *visible and darker* design patterns are commonly employed. *Visible dark patterns* are user interface (UI) and user experience (UX) practices that are easily identifiable from a regulatory and auditing perspective (e.g. through sweeps, investigations, etc.), and have relatively recognizable effects on user decision-making. In contrast, *darker patterns* refer to practices that are forced upon the user, with information that is hard to understand or inaccessible, as well as the lack or hiding of information. In contrast, *darker* patterns refer to practices that are forced upon the user, with information that is hard to understand or inaccessible, as well as the lack or hiding of information. Both *visible* and *darker* patterns can be detected and sanctioned by enforcers, though visible patterns are easier to identify and address. It is important to recognize the need for scrutiny of both *visible* and *darker* patterns to ensure transparency and accountability in UI and UX design practices. To achieve this, regulatory enforcement decisions should explicitly address deceptive design techniques and contribute to the development of a more trustworthy digital environment, thereby strengthening consumer and data protection jurisprudence.

Our analysis did not reveal a high prevalence of the *darkest dark patterns*. As previously noted by the OECD report[200], this may indicate either possible gaps in available evidence and enforcement capacity. The darkest dark patterns detection remains an enforcement challenge for regulators. System architecture patterns have the potential to negatively impact a large number of users, yet their manipulative effects are not always immediately apparent. Findings suggest that current enforcement decisions may not adequately address the problem of unobtrusive, hidden-from-view practices. Detection and auditing are typically left to activists and researchers, as they require significant technical resources. Therefore, regulators should incorporate technical expertise from computer science and other relevant domains into their oversight and design practices. By doing so, regulators can more effectively detect and prevent the use of dark patterns, including the most insidious and harmful ones. We believe that increasing the detection and enforcement of such practices is crucial to deterring the use of the *darkest* patterns.

While decisions rendered by regulators typically do not reference[201] dark patterns explicitly, they should name and denounce them in order to reinforce the message that dark patterns are not allowed and will be sanctioned.

[200] OECD Report, N153, above.

[201] So far, the first and only decision explicitly mentioning dark patterns was issued by the Italian DPA against Ediscom, and relates to a "visible" dark pattern type, focused on the UI afforded by the controller. The practice refers to the fact that the data controller adopted unclear communication models with regard to the graphic design of the interfaces and the procedures for carrying out the process of registering for the service, and configured the dark patterns of false hierarchy, nagging and obstruction. The decision reads accordingly "In some of the portals examined, during the registration process the interested party was asked to express a specific consent regarding the processing for Ediscom's marketing purposes and the communication to third parties for marketing purposes. If one of the two boxes was not selected, a pop-up was presented which highlighted the lack of consent and presented a clearly visible button for accepting the treatment. The link to continue without accepting was placed at the bottom, outside the pop-up, in simple text (without the graphic format of the button) written in a smaller font than the rest of the text and, being superimposed, not very visible. The pop-up proposition had no use for carrying out the registration process but evidently represented a further attempt to obtain the user's consent despite the fact that he had already clearly expressed his will in the previous screen. This attempt, in addition to unnecessarily aggravating the enrollment process, was characterized by a greater opacity in the ways in which the consent request was presented, increasing the probability that the interested party would give his consent not by conscious choice but rather because he was misled or in the

Accordingly regulators should explicitly refer to dark patterns in their enforcement decisions to underscore their illegality and importance of preventing manipulative practices.

The use of deceptive design is widespread among both large and small organisations, and the regulatory decisions related to such practices must be made widely available. Regulators could continue to shine light on dark patterns by publishing and promoting enforcement of dark patterns-related decisions as a means of achieving general deterrence against online manipulation. Making this information widely available (the actors involved, the practices utilised, and the sanctions imposed) has a twofold effect: organisations will be able to factor the risk of adoption of similar practices and its sanctions into their business calculations, and policymakers can be aware of the true extent of the enforcement or penalties imposed by dark patterns practices and act preemptively when detecting similar practices.

Enforcement provides a mechanism for assessing the legality of manipulative design practices on a case-by-case basis, differentiating between those that infringe upon the law and those that do not. This approach is particularly relevant in high-profile cases that could affect a large number of consumers. Rather than implementing a blanket ban on dark patterns, which could potentially stifle innovation in product and service design, an enforcement-based approach is preferable for deterring their use. Nevertheless, it is important to recognize that content, functionality, and design of user interfaces and user experience evolve rapidly, making it challenging for enforcers to keep pace with prohibited designs. Continual case law and regulatory decisions will be necessary to evaluate new designs, as any specific prohibitions in the DSA and DMA regulations may quickly become outdated. In addition, enforcers should take a forward-looking approach to all layers of deceptive design, anticipating trends and their societal implications, as well as potential impact on regulations. By adopting this approach, regulators can stay ahead of the curve and ensure that their response to manipulative design practices remains effective and relevant.

The Digital Services Act (DSA), the Digital Markets Act (DMA), and the Data Act proposal include specific prohibitions on dark patterns that target specific concepts such as autonomy, and influence types such as manipulation, impairment, deception, and distortion (among others). These have a rich semantic density and impact several interdisciplinary fields such as cybersecurity, philosophy, computer science, human-computer interaction (HCI), ethics, and others. To ensure legal certainty, the EU Commission needs to provide proactive guidelines on how to interpret these concepts within the context of the DSA, DMA and Data Act. Regarding the DSA, this regulation needs to be read in a manner that includes *visible* and *darker* patterns, but also patterns that do not regard the classical graphic user interface, such as voice and haptic interfaces, and augmented and virtual reality practices. Moreover, we recommend that the DSA's scope needs to account for emerging types of dark patterns, such as personalized hypernudges or human-robot manipulation practices. Regarding the AI Act proposal, we consider that if a given AI system deploys ML and generates UI-based content, or recommendations at UI-level, then such a system will be covered by the AI act. In this scenario, the AI act has the potential to cover darkest dark patterns. By banning the use of AI-powered "dark patterns" that are designed to manipulate or deceive users and prohibiting their use in high-risk AI systems, the proposed AI Act promotes the responsible and ethical use of AI.

Moreover, it is not yet clear when the DSA and GDPR applies, or when the DSA and UCPD applies, due to the exception given in Article 25(2) that exempts practices that are “without prejudice” already covered by these legislations. Such undefinition on the scope of applicability of existing vs forthcoming laws can generate material competence conflicts. There is a need for additional guidance on the relationship between legal norms, their scope of application whenever one or more laws are applicable.

rush to conclude the process. A similar setting was found in the screen presented to the user to invite him to provide the data of other subjects potentially interested in subscribing to the services (...). Faced with invitation messages written in bold and fields with asterisks (even if in fact optional), the option "...or skip" - which should be an alternative to the "continue" button - was shown at the bottom of the page in much smaller font and with completely different graphics compared to the "continue" option”. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014, consulted on 27/04/2023.