European Journal of Law and Technology, Vol. 15 No. 1 (2024)

EJLT European Journal of Law and Technology

Dark Patterns, Enforcement, and the Emerging Digital Design *Acquis*: Manipulation beneath the Interface

Mark Leiser and Cristiana Santos[*]

Abstract

The term 'dark patterns' is commonly used to describe manipulative or exploitative 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 focused on establishing classifications, definitions, constitutive elements, and typologies of dark patterns across different fields. Regulators have responded to these dark patterns with several enforcement decisions related to data protection, privacy violations, and rulings protecting consumers. By analysing such enforcement decisions, we conclude that this 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 the AI Act are critiqued for their suitability to regulate deceptive design over the entirety of the deceptive design visibility spectrum.

Keywords: dark patterns, deceptive design, enforcement, data protection, consumer protection, HCI.

[*] Mark Leiser is affiliated at Vrije Universiteit Amsterdam; Cristiana Santos is affiliated to the School of Law, Utrecht University. The authors would like to thank Harry Brignull and Kosha Doshi who help us run the deceptive patterns enforcement database and its associated website (https://deceptive.design).

1. Introduction

The term 'Dark patterns',[1] or 'deceptive design', commonly refers to design practices that manipulate[2] or exploit users to achieve specific outcomes, often at the expense of their autonomy, decision-making, or choices.[3] The use of dark patterns has become a growing concern. The response to dark patterns has evolved from theoretical problem-based academic work[4] and behavioural studies[5] to active enforcement by regulatory bodies worldwide.[6] The amalgamation of these results yielded a framework for policy-oriented interventions delineating the perils posed by dark patterns and associated deceitful design techniques. Various regulatory bodies, including the US Federal Trade Commission (FTC),[7] the UK Competition and Market Authority (CMA),[8] the European Commission,[9] the European Data Protection Board

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

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

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

[4] C. Bösch et al., '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; L. Fritsch et al., 'Privacy Dark Patterns in Identity Management' [2017] Lecture Notes in Informatics (LNI) 93; M. Leiser and W. Yang, 'Illuminating manipulative design: From "dark patterns" to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive' (12 November 2022) https://doi.org/10.31235/osf.io/7dwuq accessed 11 April 2023.

[5] European Commission, Directorate-General for Justice and Consumers, F. Lupiáñez-Villanueva et al., 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.

[6] See M. Leiser, C. Santos, and K. Doshi (2023), Dark Patterns Enforcement Database (https://deceptive.design).

[7] 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.

[8] 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.

[9] 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.

(EDPB),[10] and the Organisation for Economic Cooperation and Development (OECD),[11] issued high-profile policy guidance on distinct varieties of dark patterns that exhibit significant overlap with definitions put forth in academic literature.[12] 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,[13] Digital Markets

[10] 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 autonomy, 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.

[11] OECD, ‘Dark commercial patterns‘, *OECD Digital Economy Papers*, No. 336 (OECD Publishing, 2022) https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en accessed 16 March 2023.

[12] 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 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 https://doi.org/10.1145/3411764.3445779; M. Nouwens et al., ‘Dark Patterns After The GDPR: Scraping Consent Pop-Ups And Demonstrating Their Influence’ (Association for Computing Machinery, 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; M. 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*; M. 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; L. Strahilevitz et al., Subcommittee report: Privacy and data protection, Stigler Center Committee for the Study of Digital Platforms 22–23 (2019); M.R. Leiser and M. Caruana, ‘Dark Patterns: Light to be found in Europe’s Consumer Protection Regime’ (2021) 10(6) *Journal of European Consumer and Market Law* 237–251

[13] 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).

Act,[14] Data Act,[15] and AI Act.[16] The incorporation of the term into Guidance Documents[17] and Codes of Conduct,[18] and the development of 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.[19] 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.

The present means of studying deceptive design and its legal implications centres around a descriptive and classificatory[20] approach that identifies malicious strategies and assesses their legality within the confines of concrete contexts and specific legislative instruments. However, this article contributes two-fold to the state-of-the-art research of dark patterns. Firstly, it 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),[21] the e-Privacy Directive (ePD),[22] and the Unfair Commercial Practices Directive (UCPD),[23] which are working to establish legal standards for transparent and fair data processing and marketing practices.[24] Considering dark pattern deterrence requires the execution of enforcement and penalties, this work focuses on scrutinising regulatory cases that can be classified as dark patterns. It marks the first attempt to investigate this area of

[14] 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).

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

[16] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (consolidated version of 26 January 2024).

[17] 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.

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

[19] 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/.

[20] C. M. Gray, N. Bielova, C. Santos, and T. Mildner, An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action. 1, 1 (September 2023), forthcoming at the Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24).

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

[22] Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the e-Privacy Directive').

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

[24] Liability claims (for example, the proposed Artificial Intelligence Liability or the provisions under the UCPD) are hence excluded from the analysis of this paper.

study. Therefore, section 2 below analyses regulatory decisions, concluding that there is a tendency among regulators to focus exclusively on dark patterns present in online user interfaces (UI) and user experiences (UX) while neglecting the more insidious and covert patterns embedded within system architectures. We advance our discussion by proposing a three-tier visibility threshold for dark patterns:

- *Visible dark patterns* are open, evident and overtly manipulative design practices that exert readily recognisable effects on user decision-making and are more easily recognisable by regulators and auditors. Examples include nagging, preselection, and other techniques best described as 'in-your-face' patterns.
- *Darker patterns* are more subtle and elusive, and refer to covert practices not immediately discernible to end-users, necessitating further scrutiny by regulatory authorities, expert auditors and technical experts. Examples include design techniques that make essential aspects of contract formation (e.g., terms and conditions and privacy policies) difficult to find or navigate, obscuring the ability to withdraw consent behind the scenes of the UI, and requiring multiple clicks and user effort to navigate.
- The *darkest patterns* represent the most insidious forms of digital manipulation, characterised by their sophisticated algorithmic foundation. These patterns are designed to exploit cognitive biases, personalise experiences through hyper-nudging, and operate on both individual and collective levels, often beyond the immediate perception of users. The main distinction within these patterns lies between deterministic and stochastic approaches:
    - *Deterministic patterns* are built on complex coding and system architecture, utilising user behavioural data and preferences to drive outcomes that are not, in the end-users' interests and are often hidden from them. These patterns are precisely engineered to achieve specific, undesirable outcomes for users, making their detection possible only through in-depth technical analysis. This approach relies heavily on targeting cognitive biases and personalising manipulation, using detailed user data to craft experiences that users are likely to follow, even against their best interests.
    - *Stochastic (non-deterministic) patterns* involve systems that operate as black boxes, where the reasoning behind their outputs is unclear, and outcomes for identical inputs can vary. Often based on machine learning (ML) or other statistical methodologies, these systems adapt and change unpredictably for both users and developers. This category of dark patterns extends the manipulation to a collective level, affecting user groups and communities in ways that are not immediately recognisable and often operate beyond the surface level of interaction.

Both darkest patterns engage deeply with Willis's 'Deception by Design'.[25] By leveraging algorithmic processes, these patterns target individual cognitive biases and manipulate collective behaviours, making their detection and understanding a complex challenge. The key to distinguishing these patterns lies in their foundation: whether they are deterministic, with a clear, albeit hidden, logic behind their manipulation, or stochastic, presenting unpredictable and often inexplicable outcomes. Recognising the multifaceted nature of these manipulative practices is essential in developing effective countermeasures and fostering digital environments that respect user autonomy and consent.

This three-tier visibility threshold does not imply a degree of harm or severity between the different types of dark patterns; it instead refers to the detectability thereof. Section 2 concludes that the GDPR, ePD and UCPD sufficiently address visible and darker patterns, but still need to address the darkest patterns adequately.

Secondly, this paper scrutinises the nascent digital regulatory framework, encompassing the Digital Services Act (DSA), Digital Markets Act (DMA), Artificial Intelligence Act, and Data Act, which explicitly addresses dark patterns.[26] We explore the challenges posed by such legislation, focusing on the visibility spectrum. Section 3 revisits and expands upon the 'user interface' concept within digital systems, highlighting its inadequacy in capturing non-visual interactions and their potential for manipulative designs. It advocates for regulatory oversight to encompass the entire 'system architecture' to ensure digital systems' compliance with the law.

Section 4 examines the EU's recent and prospective regulatory strategies towards dark pattern practices, specifically through the DSA, DMA, AI Act, and Data Act. The analysis critiques the EU's obligations, prohibitions, and mitigation measures within its developing digital regulatory corpus. The concluding part of this section questions the adequacy of the current regulatory framework, arguing for a revision of the digital regulatory corpus to govern dark patterns across the full visibility spectrum effectively.

Section 5 offers guidance for regulators on addressing dark patterns within the enforcement of the EU's evolving digital regulatory framework.

2. Enforcement against Dark Patterns

The GDPR, the e-Privacy ePD, and 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

[25] L. E. Willis, 'Deception by design' (2020) 34(115) *Harvard Journal of Law & Technology*.

[26] Liability claims (e.g., the proposed Artificial Intelligence Liability or the provisions under the UCPD) are hence excluded from the analysis of this paper.

responsibilities, initiating legal actions under relevant laws against dark patterns without explicitly designating them as such.[27]

In the following sections, we present our analysis of the enforcement decisions made by data protection and consumer regulators.[28] Our methodological approach involved analysing the decisions per legal domain, separating them into data protection (section 2.1), and consumer law (section 2.2). We selected the practices that may relate to known dark pattern taxonomies.[29] Our analysis of regulatory decisions reveals that deceptive design exists on a spectrum, ranging from *visible* dark patterns readily observable by any stakeholder auditing them to less visible auditable 'darker' patterns and ultimately to completely invisible 'darkest' patterns. Therefore, we present our findings from the collected decisions according to this visibility spectrum. Tables 1 and 2 illustrate the distribution of regulatory consumer and data protection cases based on the visible spectrum and per dark pattern type.

2.1 Enforcement from a Data Protection Perspective

Our thorough examination of regulatory decisions indicates that although the GDPR and e-Privacy Directive do not expressly mention dark patterns, these legislative frameworks play a fundamental role in their enforcement.

[27] C. Santos and A. Rossi. The emergence of dark patterns as a legal concept in case law (2023) https://policyreview.info/articles/news/emergence-of-dark-patterns-as-a-legal-concept accessed 8 February 2024.

[28] 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 GDPR hub repository (https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub), which provides cases in original languages and automated English translations. We have read the summary decisions to interpret whether they could be related to dark pattern practices. During this process, we found more decisions related to data protection since it was easier to find them in contrast to consumer law-based decisions. 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 quantify how many decisions relate to dark patterns.

[29] The labelling of certain practices identified in the decisions as dark patterns relied upon the authors' 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 (nagging, obstruction, forced action, interface interference, sneaking, social proof, urgency), cf. OECD (n 11) 53 https://doi.org/10.1787/44f5e846-en.

2.1.1 Visible Dark Patterns

Notably, the most prevalent dark patterns involve preselection, obfuscation of refusal and withdrawal mechanisms, and bundled practices. 'Pre-checked boxes'[30] have decreased in recent years due to explicit judicial prohibitions[31] and further guidelines from the EDPB[32] and data protection authorities (DPAs).[33] Instead, users are presented with default options for consent[34] for data-sharing with third parties under advertising targeting or commercial communication. These are called 'preselection' practices or *defaults* since users are tricked or forced into sharing more personal information than desired.[35]

Several decisions report using 'bundling or tying practices' 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.[36] Sometimes,[37] using a particular service requires users to consent to data processing. Users may also be subjected to e-marketing without choice.[38] Users are also asked to consent for multiple unrelated purposes (including advertising) without any meaningful granular choice[39] or to consent to process tracers that serve several purposes.[40] Such practices infringe on users' free and specific consent and are considered dark patterns of 'forced action'[41] as users are tricked or forced into sharing more personal information than desired.

The decisions made by the DPAs reveal instances of 'obstructive refusal and withdrawal options'. These decisions refer to cases where users had to perform many actions relating to deactivating or turning off their settings[42] and selecting more

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

[31] Judgment in Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbande – Verbraucherzentrale Bundesverband eV v Planet49 GmbH*.

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

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

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

[35] OECD (n 11).

[36] *French v Google LLC*, 2019; *Finnish DPA v Polar Oy*, 2022.

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

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

[39] Arts. 4(11), 7(3) GDPR.

[40] *French DPA v Microsoft*, 2022.

[41] OECD (n 11).

[42] *French DPA v Apple*, 2022.

privacy-preserving options (without advertising being enabled). Several cases[43] reported how cumbersome or impossible it was to reject non-necessary trackers, such as third-party advertising trackers. Examples illustrate a lack of control panels for rejecting consent, inadequate options for declining at the second layer of a cookie banner, and the need to configure browser settings or visit third-party websites to deny each partner separately). Other cases[44] report that data subjects could not withdraw consent regarding cookies or cases[45] wherein users could not withdraw consent as quickly as it was given (e.g., using a link in the commercial information; demanding to provide the reason for withdrawing consent). Some decisions[46] 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. A few cases[47] 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 'obstruction', denoting asymmetry in the 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.[48] Suppose users do not master the language in which the privacy policy information is given. In that case, they will be unable to review it and, therefore, likely not be aware of how data is processed, which is especially severe when a website addresses a child. The EDPB labels this practice a 'language discontinuity'[49] type of dark pattern.

[43] *French v Facebook Ireland Limited*, 2021; *Spanish DPA v Happy Friday, S.L.*, 2019; *Spanish DPA v Lia's Clothes*, 2021; *Spanish DPA v Ramona Films S.L.*, 2022; *Spanish DPA v Iberia*, 2020; *Spanish DPA v Marbella Resorts*, 2021; *Spanish DPA v Radio Popular*, 2021; *Spanish DPA v FDM*, 2020; *Spanish DPA v FurnishYourSpace*, 2020; *Spanish DPA v Twitter*, 2021; *Spanish DPA v The Washpoint SL*, 2020; *Spanish DPA v The Washpoint SL*, 2020; *Spanish DPA v Facua*, 2020; *Danish DPA v DGU Erhverv A/S*, 2020; *Danish DPA v JAVA*, 2020; *Spanish DPA v X*, 2020; *Finnish DPA v Traficom*, 2020; *French DPA v Tiktok* 2022; *Danish DPA v DMI*, 2020; *Spanish DPA v Miguel Ibáñez Bezanilla, S.L.*, 2020; *Spanish DPA v Canary Click Consulting website*, 2020; *Belgian DPA v Toerisme Vlaanderen*, 2O22; *Norway DPA v Grindr LLC*, 2021; *French DPA v Microsoft*, 2022; *Belgian DPA v Youronlinechoices*, 2022.

[44] *Spanish DPA v X website*, 2022.

[45] *Belgian DPA v Roularta Media Group*, 2022; *Spanish DPA v X*, 2019; *Polish DPA v ClickQuickNow Sp.z o.o*, 2019.

[46] *Belgian DPA v Telenet*, 2021; *Italian DPA v Wind Tre SpA*, 2020; *UK DPA v Colour Car Sales Limited*, 2021.

[47] *Spanish DPA v Cooltra Motosharing S.L.U.*, 2019.

[48] *French DPA v Tiktok*, 2022; *Austrian DPA v Co Material GmbH*, 2021; *Spanish DPA v AAA Just Landed S.L.*, 2019.

[49] 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.

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'[50] 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.'[51] This repetitive and obstructive communication disrupts users. It infringes the principles of lawfulness and fairness. Moreover, these behaviours might entail the dark patterns of 'nagging'.[52]

2.1.2 Darker Patterns

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[53] is essential to enable users to make informed choices. For instance, specific names[54] that are given to options were framed as unclear (e.g., 'manage data settings' button or 'we use cookies to optimise the users' experience); other cases report a lack of clarity and understandability of essential information that does not allow users to sufficiently understand the particular consequences of the processing for them[55] on the pursued description of purposes, the data controller, collected data, the legal basis for specific purposes, retention periods, joint controllers, etc.[56]

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

[51] *Italian DPA v Enel Energia Spa*, 2021; *UK DPA v We Buy Any Car Limited*, 2021; *Italian DPA v Wind Tre SpA*, 2020; *Norway DPA v Komplett Bank ASA*, 2021; *UK DPA v Unite the Union*, 2021.

[52] OECD (n 11).

[53] Art. 12 GDPR.

[54] *French v Facebook Ireland Limit*ed, 2021; *Spanish DPA v FurnishYourSpace*, 2020.

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

[56] *Danish DPA v DMI*, 2020.

Other decisions report that the cookie banner only offered generic information[57] or that the privacy policy was vague.[58] Such practices can be related to the dark pattern of 'obstruction'. 'Misleading practices' were also observed in the analysed decisions. These include incorrect categorisation of third-party cookies as technically essential. Consequently, when users unchecked the relevant boxes or clicked 'reject all,' non-essential cookies remained; the company used some cookies for a purpose not listed in its privacy policy[59] or the use of a cookie serving several purposes.[60] Other decisions denounce that data protection information was in tiny print and barely legible.[61]

Moreover, cases expose that privacy policies state misleading information[62] (e.g., stating that personal data would only be used for 'strictly necessary purposes' and that marketing was included in the data processing.[63] Other cases divulge the use of cookies for a purpose not listed in its privacy policy.[64] Finally, cases denote the use of misleading and complicated language[65] (e.g., 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 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 are associated with dark 'hidden information' patterns 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 practices where users were not informed about data processing purposes (and how to reject them),[66] and users were not informed about third-party recipients with whom data was shared (for advertising purposes).[67]

'Forced practices' demonstrating user consent exploitation and personal data manipulation were sanctioned when personal data was processed before consent

[57] *Spanish DPA v FDM*, 2020; *Spanish DPA v Bodegas Dinastía, S.L.*, 2020.

[58] *Spanish DPA v Happy Friday, S.L.*, 2019; *UK DPA v Emailmovers Limited*, 2021; *Swedish DPA v Klarna Bank AB*, 2022; *Belgian DPA v Y Housing Company*, 2020; *Czech DPA v Television Operator*, 2021.

[59] *French DPA v Carrefour Group*, 2020.

[60] *French DPA v Microsoft*, 2022.

[61] *Hungarian DPA v Magyar Éremkibocsátó Kft*., 2022.

[62] *Hungarian DPA v Infotv*, 2022; *Belgian DPA v Toerisme Vlaanderen*, 2O22; *Spanish DPA v Iberia*, 2020.

[63] *Spanish DPA v Canary Click Consulting website*, 2020; *Spanish DPA v Esclora Proyectos*, 2020.

[64] *French DPA v Carrefour Group*, 2020.

[65] *Spanish DPA v FurnishYourSpace*, 2020; *Spanish DPA v Facua*, 2020.

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

[67] *Norway DPA v Grindr LLC*, 2021.

was given[68] and when non-essential trackers (such as advertising and third-party analytical tools) were deposited on users' computers without prior consent.[69] Decisions also report[70] that when consent is withdrawn, unnecessary trackers are loaded. In some instances,[71] non-essential cookies increased in number despite the user's attempts to reject them. Moreover, decisions refer to practices where cookies were stored after the withdrawal of consent.[72] Such trackers encompassed statistics, social network cookies, and advertising cookies from third-party domains. Other practices related to third-party cookies were incorrectly categorised as technically essential, and consequently, when users unchecked the relevant boxes or clicked 'reject all', non-essential cookies remained.[73] Such practices influence the users' freely given consent, which should be meaningful and unburdened by coercion, pressure, or dependence on unnecessary processing purposes. These online tracking practices can be attributed to the dark 'forced action' pattern.

Further concerns arise due to 'design choices that fragment data protection information', making it difficult to access the information required to make informed decisions. We found cases where relevant information (e.g., on purposes, retention periods, etc.) was difficult to find and excessively spread 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.

[68] *Italian DPA v Uber Italy srl*, 2022; *Spanish DPA v Banco Bilbao Vizcaya Argentaria, SA*, 2020.

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

[70] *Belgian DPA v Rossel & Cie*, 2022.

[71] ibid.

[72] ibid; *Polish DPA v ClickQuickNow Sp.z o.o*, 2019; *French DPA v Societe du Figaro*, 2021; *Spanish DPA v FDM*, 2020.

[73] *Spanish DPA v Vueling Airlines S.A.*, 2019.

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

Table 1: Regulatory data protection cases are distributed according to the visibility spectrum and per dark pattern type

Data protection cases		
Visibility spectrum	**Identified practices in regulatory decisions**	**Related dark patterns**
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 of hidden information	Hidden information (sometimes sneaking)

2.2 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 unfair and misleading commercial practices are linked to visible and darker practices.

2.2.1 Visible Dark Patterns

Visible dark patterns include obstructive refusal and urgency claims. Obstructive refusal practices are featured in decisions that make it difficult to refuse or unsubscribe a service[75] (e.g., refuse insurance). The Norwegian Consumer Council (NCC) and other European consumer organisations filed legal complaints against Amazon for preventing consumers from unsubscribing from its Prime service.[76] Other cases referred to urgency messaging claims,[77] such as misleading countdown clocks in the online architecture to pressure consumers into purchasing. For example, following a coordinated CPC network action, two giant online platforms, Booking.com and Expedia, improved the presentation of their accommodation offers, aligning them with EU consumer law.[78]

2.2.2 Darker Patterns

Darker patterns consist of forced practices, hidden costs, and lack of hidden information, which are less detectable. Some 'forced practices' that fall under the 'forced action' category have been reported in some decisions. These practices include binding consumers to premium subscriptions without their knowledge after a free trial period,[79] prompting users to register on a platform without disclosing that their data will be used for commercial purposes[80] and unclear auto-renewal policies that may result in users being charged for services they no longer use.[81] In specific decision-making contexts, consumers were faced with 'hidden costs'. Some decisions referred to the fact that certain subscriptions entailed charges[82] or costs not mentioned in the base price and had optional extras often pre-selected. Their presence only becomes evident after the purchase, contributing to the dark 'sneak into basket' pattern. A 'lack of adequate and essential information' was observed in other decision-making situations essential to making informed choices.[83] For example, travel insurance policies that cover the risk of cancellation or websites claiming price comparisons[84] do not display business names or disclose fixed charges

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

[76] 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/.

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

[78] 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.

[79] *AGCM v Edates*, 2016.

[80] *ICA v Facebook*, 2018.

[81] *CMA v Microsoft's Xbox Live Gold and Game Pass Products*, 2022.

[82] *CMA v Adaptive Affinity*, 2011.

[83] *CMA v Microsoft's Xbox Live Gold and Game Pass Products*, 2022.

[84] *CMA v Heating oil price comparison websites - Fuelfighter.co.uk; Boilerjuice.co.uk; Cheapheatingoil,* 2011.

to consumers.[85] In some instances, properties were marketed as 'discounted' without revealing that the price was based on a standard rate provided by the accommodation provider.[86] Such practices, which relate to the dark pattern of 'hidden information' and 'sneaking', can undermine consumers' autonomy and decision-making, leading to adverse outcomes.

Table 2: Distribution of regulatory consumer and data protection cases according to the visibility spectrum and per dark pattern type

Consumer law cases		
Visibility spectrum	**Identified practices in regulatory decisions**	**Related dark patterns**
Visible	Obstructive refusal	Obstruction
	Urgency claims	Urgency
Darker	Forced practices	Forced registration
	Hidden costs	Sneaking (hidden costs)

2.3 Synthesis

From the enforcement analysis, we confirm that visible and darker design patterns are commonly employed by digital services, corresponding to practices occurring at the UI and UX levels.

Such dark pattern practices are captured within the generally phrased obligations that apply to dark patterns. Data protection law triggers legal protection against dark patterns through overarching principles (fairness, transparency, data protection of data by default and design, etc.) and consent legal requirements that are not specific to dark patterns and regard individual harms of affected data subjects. The UCPD prohibits certain professional practices that would lead consumers to make decisions they otherwise would not have taken.

[85] *CMA v Expedia*, 2017.

[86] ibid.

3. Digital Design Across the Spectrum of Visibility

As highlighted in the introduction, the enforcement focus relies mainly on visible dark patterns in the online graphical interface and interaction with digital services. In this section, we propose to extend the current understanding of online interfaces in section 3.1, as it is becoming evident that most dark pattern practices are embedded in the underlying code. Accordingly, section 3.2 focuses on the role of regulatory oversight in controlling dark patterns and deceptive design practices built into the system architecture.

3.1 Rethinking the User Interface

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 UX.[87] The UX encompasses users' overall experience when interacting with a digital product or application. It includes usability, accessibility, performance, and user satisfaction.[88]

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.[89] The authors, returning to a literal interpretation of the interface as a surface, opened fresh avenues for contemplating interactive technologies and faceless interactions (e.g., home assistants like Alexa, Google Home, smart speakers,[90] and the multitude of 'Internet of Things' devices on the market, etc.).[91]

The authors identified two groups of modalities: '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 pre-eminent surface. Nevertheless, there is a

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

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

[89] L.-E. Janlert and E. Stolterman, '9 Faceless Interaction' in *Things That Keep Us Busy: The Elements of Interaction* (MIT Press, 2017) 155–171.

[90] S. De Conca, The Present Looks Nothing Like the Jetsons – Deceptive Design in Virtual Assistants and the Protection of the Rights of Users http://dx.doi.org/10.2139/ssrn.4412646.

[91] M. Kowalczyk et al., '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.

considerable risk of consequences in ‘surface-free’ interactions. As ‘surface-free’ modalities may add a layer of complexity, this carries implications for the design of digital systems and the UX. 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 interface-less interactions where manipulative design practices occur beyond the traditional graphical UI of digital systems. The hyper-personalisation of voice assistants has already been deployed in the market.[92]

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, 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 beyond practices detected in enforcement cases so far.

3.2 Systems of Manipulation and the Darkest Patterns

Both the UI and UX are heavily influenced by the design of the online interface and the efficiency of the underlying ‘system architecture’, i.e., the structural design of a digital product or application.[93] However, this separate treatment must be revised to reflect modern design techniques. Boroji posits that designers adopt an ‘iceberg model of design’ made up of interconnected surfaces, skeletons, structures, scope, and strategy layers. For Boroji, the surface is just the tip of the iceberg.[94] By comprehending the interplay among these components, designers and developers can facilitate more nefarious patterns embedded deep in the system architecture.[95]

[92] ‘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.

[93] A. Stuart, ‘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).

[94] H. 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.

[95] For an example of common design techniques, see A. 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.

As it typically encompasses the data flow, processing, storage, and communication between various components, a system would be far more efficient at manipulating users through hyper-nudging at scale or engaging users with hyper-personalisation[96] if the entire architecture were designed for this end.

Deciding whether the darkest pattern has been used is challenging, and the regulatory case analysis in the preceding sections did not show specific enforcement decisions involving the darkest patterns. The darkest patterns are detective design techniques purposely integrated into an online service's system architecture (SA) or code level and not on the UI/UX. The system architecture constitutes the structural design of a digital product or application.[97] Developers may use ML algorithms to analyse user behaviour and create hyper-nudges or recommendations that steer users towards choices not in their best interests. These algorithms[98] may be designed to optimise engagement or revenue rather than user well-being, leading to a system architecture that prioritises business goals over user needs.

Scholarship from algorithmic design classifies these as 'deterministic algorithms'.[99] An example of a 'complex deterministic algorithm'[100] is a highly personalised recommendation considering multiple factors, including user behavioural data and preferences. A highly personalised recommender system achieves the design objective: the user acts upon a given recommendation that would not have been taken without the design. An outside auditor could still inspect such algorithms and subject them to regulatory oversight. On the other hand, 'non-deterministic dark patterns'[101] involve non-deterministic algorithms and ML systems or other opaque statistical methods that are difficult to understand.[102] The system is purposely designed to give different outputs to the same inputs. These patterns involve

[96] '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

[97] Stuart (n 93).

[98] 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.

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

[100] ibid.

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

[102] D. E. Knuth, 'Estimating the efficiency of backtrack programs' (1975) 29 *Mathematics of Computation* 121–136, 129.

techniques such as 'dark data collection',[103] 'shadow profiling',[104] or data-sharing practices that are not visible to users but impact their privacy or decision-making. Detecting non-deterministic patterns requires insider information and is most difficult to detect, audit or regulate.

Using opaque algorithms and ML techniques in the darkest patterns seriously threatens user autonomy, control over personal data, and data subject rights,[105] 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 practices. One, however, involves Google's practice of saving users' location data even after location tracking had been turned off in the privacy settings. Despite users turning location data off, Google's architecture and code were programmed to store time-stamped location data automatically without asking.[106]

The Dutch Authority for Consumers and Markets (ACM) has highlighted the risk of embedding algorithms in the system architecture to analyse consumer behaviour, preferences, and previous interactions to exploit the consumer decision-making process by manipulating the options presented to them.[107] These bubbles isolate users from diverse perspectives and reinforce their existing beliefs to benefit the platform.[108] The darkest patterns embedded in the system architectures can exploit psychological biases like intermittent rewards and variable reinforcement schedules to encourage addictive behaviour and increase user engagement.[109] Addiction techniques like feedback loops can be implemented into the system architecture through various design and development strategies that exploit psychological

[103] R. Van Loon, '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

[104] L. Aguiar, C. Peukert, M. Schäfer, and H. Ullrich. 'Facebook shadow profiles' arXiv preprint arXiv:2202.04131 (2022); T. Moseley, A. Shye, V.J. Reddi, D. Grunwald, and R. Peri, Shadow profiling: Hiding instrumentation costs with parallelism, in *International Symposium on Code Generation and Optimization* (CGO '07, March 2007) 198–208. IEEE.

[105] S. Barros Vale and G. Zanfir-Fortuna, Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities (FPF, 20220 https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf accessed 29 March 2023.

[106] Google pays nearly $392 million to settle sweeping location-tracking case (14 November 2022), https://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 accessed 25 April 2023.

[107] 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.

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

[109] M. Kumar and A. Mondal, 'A study on Internet addiction and its relation to psychopathology and self-esteem among college students' (2018) 27(1) *Industrial Psychiatry Journal* 61–66.

principles and encourage addictive behaviour.[110] These techniques aim to increase user engagement, retain users, and maximise the time they spend on a platform or application. Standard addiction techniques can be integrated into the system architecture.[111]

A system architecture can be designed to exploit psychological principles that encourage addictive behaviour and increase user engagement.[112] 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.[113] Platforms can create a sense of anticipation and excitement by providing users with unpredictable rewards or positive reinforcement at varying intervals.[114] To create these psychological stimuli, algorithms must be implemented in the system architecture that rewards 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 a 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 will receive the next 'like' or comment.[115]

Developers can also encourage continuous content consumption by automatically loading new content as users reach the end of a page or a video. This tactic can be implemented 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. A system architecture that incorporates biased algorithms can hurt users.[116] For example, a recommendation algorithm that

[110] D. B. Dillard-Wright, '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.

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

[112] M. Flayelle, D. Brevers, D. L. King et al., 'A taxonomy of technology design features that promote potentially addictive online behaviours' (2023) 2 *Nature Reviews Psychology* 136.

[113] G. Collins, '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.

[114] J. 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.

[115] B. Barnhart, '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.

[116] The FTC emphasises such negative and discriminatory effects in its Joint Statement on AI: 'We already see how AI tools can turbocharge fraud and automate discrimination, and we won't

prioritises content based on popularity or engagement may inadvertently amplify controversial or harmful content, skewing users' perception of reality.

3.3 Synthesis

Section 3.1 purposely adopts a broad UI definition that aims to include interface-less interactions. In contrast, section 3.2 relates the UI and UX, emphasising the complex relationship with the system architecture of digital services. The following section analyses digital *design acquis* considering these conceptual foundations.

4 The New Digital Design *Acquis* and the Visibility Spectrum

This section scopes emerging legislation crafting dark pattern-specific provisions and discusses its challenges from the perspective of the visibility spectrum. Herein, we account for the DSA and the DMA alongside the Data and AI Acts. Particular attention is given to the DSA, our discussion revolving around the concept of the online interface and the AI Act for its potential to cover the darkest patterns.

4.1 The Digital Services Act

The DSA[117] is a legislative instrument regulating online intermediaries operating within the EU Single Market. The personal scope includes[118] 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.[119]

hesitate to use the full scope of our legal authorities to protect Americans from these threats ... Technological advances can deliver critical innovation—but claims of innovation must not be cover for lawbreaking. There is no AI exemption to the laws on the books, and the FTC will vigorously enforce the law to combat unfair or deceptive practices or unfair methods of competition' https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-chair-khan-officials-doj-cfpb-eeoc-release-joint-statement-ai, and https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf accessed 27 April 2023.

[117] 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.

[118] Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413 accessed 8 February 2024.

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

Article 25(1) DSA prohibits platforms[120] from designing, organising, or operating their online interfaces[121] 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'. Article 25 of the DSA applies explicitly to 'online platforms'[122] and does not extend to other entities that fall within the DSA's scope. Empirical studies,[123] 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.[124] The user's decisional space is (i) *autonomy*[125] – the capacity to make one's own choices by having the competency to do so and being able to endorse the reasons for them authentically;[126] (ii) *choice* – the user's options, and (iii) *decision* – actions or behaviours that manifest former choices and are externally manifested and visible.[127]

[120] 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.

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

[122] Art. 3(m) DSA.

[123] J. Gunawan, A. Pradeep, D. Choffnes, W. Hartzog, and C. Wilson, 'A Comparative Study of Dark Patterns Across Mobile and Web Modalities' (2021) 5 (CSCW2) *Proceedings of the ACM on Human–Computer Interaction*, Article 377 https://doi.org/10.1145/3479521; L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, and A. Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception in *Proceedings of the 2020 CHI Conference*; A. Mathur, G. Acar, M. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan (n 12).

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

[125] While there is an increasing body of work defining personal autonomy, the DSA leaves the term undefined. The definition of 'autonomy' is nevertheless out of the scope of this paper. For further scholarly readings on the topic, we refer to M. Gartner, 'Regulatory Acknowledgment of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act' (2022) 8(4) *European Data Protection Law Review* 462 https://doi.org/10.21552/edpl/2022/4/6; Susser et al. refer to one who has the competencies (cognitive and affective) to consider one's choices and to act upon them: D. Susser, B. Roessler, and H. Nissenbaum, 'Technology, autonomy, and manipulation' (2019) 8(2) *Internet Policy Review*, 1–22 https://doi.org/10.14763/2019.2.1410.

[126] Art. 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 Art. 14 (Content Interference via Terms and Conditions), Art. 20 (Complaint Handling), Art. 38 (Recommender Systems), and Art. 25 (Dark Patterns).

[127] Arts. 14, 24, and 25 DSA.

Recital 67 of the DSA provides additional context and clarification on the prohibition of dark patterns of Article 25. In this context, (i) '*structure*' refers to the overall layout and organisation of an online interface or a part thereof; (ii) '*design*' refers to the visual elements of an online interface, such as colour 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 prohibits various practices. It includes those that manipulate,[128] deceive, materially distort, impair, nudge, and exploit users' choices, decision-making and autonomy. These different influence types are not clarified; accordingly, the undefined and unbound space surrounding them might trigger legal uncertainty, lack specificity and lead to different interpretations for designers, developers, regulators, and policymakers to foreground and disambiguate, each according to their pursuits.

Article 25(2) provides for 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 includes 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 the GDPR and UCPD.[129] As a result, dark patterns practices involving personal data are covered by the GDPR, and the UCPD covers all dark patterns involved in business-to-consumer transactions. However, due to the subsidiary nature of the DSA, specific dark patterns, such as infinite scroll, autoplay, and nagging practices, might not be covered by existing legislation. These practices might also include business-to-business activities not governed by the UCPD. Recently, the EU Commission initiated formal proceedings against X[130] due to the alleged 'social proof' dark pattern related to the false claim of X's blue checkmark subscriptions. Celebrity accounts, like those of LeBron James, Stephen King and William Shatner, falsely claimed they were paying for a blue check subscription when they were not. Supposedly, X used misleading information regarding the popularity of the blue subscription checks, exploiting the social proof bias. The wording adopted in Article 25(1) – 'design, organise, or operate' – seems to scope the *classical graphical user interface* (GUI). However, it seems to sidestep the darkest patterns, such as personalised hyper-nudges, human–robot manipulation, voice assistant and haptic interfaces, and augmented and virtual reality.

Moreover, it is unclear which standard a service's 'recipient' should be evaluated against. Akhurst et al. propose that the EC clarify whether such a standard should rely on the concept of the average or vulnerable user.[131] While Recital 67 mentions

[128] 'Manipulation' has not been defined yet in EU law and requires further elaboration and disambiguation regarding other influence types.

[129] OECD (n 11) 31 and Annex F.

[130] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709 accessed 8 February 2024.

[131] T. Akhurst, L. Zurdo, R. Rapparini, and C. Mautner Markhof, How should the European Union regulate dark patterns? SciencesPo (April 2023) https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/09/Dark-Patterns.pdf accessed 8 February 2024.

presenting choices in a non-neutral manner, it is unclear what 'neutral manner' means. This lack of clarity might lead to different interpretations and uncertainty, and make it difficult to enforce the provisions of the DSA.

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 adverse effects of their services on public interests, such as democracy, public health, or security.[132] These measures include transparency, oversight, accountability, and user empowerment mechanisms.[133] Regulators may fit in dark patterns-based risk mitigation measures by enforcing laws and guidelines that protect consumers from deceptive practices.[134] Some of these measures may include:

- requiring clear and conspicuous disclosure of material information
- prohibiting misleading or coercive tactics that influence user behaviour
- ensuring users have meaningful choices and control over their data and preferences
- providing users with straightforward ways to opt-out or cancel services
- monitoring and auditing compliance with privacy and consumer protection laws.

Recital 83 also refers to *risks* stemming from the

> design, functioning or use, including through manipulation, of huge 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 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 service recipients.

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 part of the 'functionalities' of an online interface or a part thereof. This would require creative judicial interpretation in the language of the Act.

The DSA is an example of risk regulation.[135] Article 35 DSA outlines various risk mitigation measures that very large online platforms and very large online search engines must implement to address systemic risks related to deceptive design. First,

[132] Art. 34 DSA.

[133] Art. 34(2) DSA.

[134] Art. 34(1)(a) DSA.

[135] R. Baldwin, M. Cave, and M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, Oxford University Press, 2012).

Article 35(1)(a) states that platforms can be directed to mitigate the risk of a deceptive design by 'adapting their services' design, features, or functioning, including online interfaces'. Second, platforms may be asked to take 'awareness-raising measures and to adapt their online interface'.

4.2 The Digital Markets Act

The DMA[136] addresses the role and unfair practices of specific online platforms that qualify as 'gatekeepers'.[137] By identifying gatekeepers, the DMA enables regulators to focus on platforms most likely to engage in dark patterns practices. Gatekeepers provide platform services, including online intermediation, search engines, social networks, video-sharing, number-independent interpersonal communication services, operating systems, cloud computing services, advertising, and more.[138]

In Article 13(6), the DMA introduces prohibitions related to dark patterns, emphasising that gatekeepers must refrain from engaging in behaviour that undermines the effectiveness of the prohibitions and obligations laid down in the regulation.[139] This prohibition includes:

- Degrading the conditions or quality of any of the core platform services provided to business users or end users who consent (under Article 5).
- Making the exercise of rights of choices unduly difficult, presentation of end-user choices in a non-neutral manner, or subversion of user autonomy, decision-making, or choice through the structure, function, or operation of a UI or part thereof. Recital 70 of the DMA emphasises these same prohibitions for gatekeepers.

However, the provisions are unclear on whether the term 'user interface' strictly refers to the interface design of a company or includes the UX 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 5(2) prohibits gatekeepers from accumulating and cross-using data without users' consent. So, consent under the DMA is defined by the GDPR and needs to be specific and freely given. Several cases in section 2.1 relate dark pattern practices of non-freely given and unspecified user consent. Finally, Recital 63 prohibits gatekeepers from making it 'unnecessarily difficult or complicated for business users or end users to unsubscribe from a core platform service', related to the dark pattern of obstruction.

[136] 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).

[137] Arts. 2(1) and 3, and recital 16 DMA.

[138] Art. 2(2) DMA.

[139] Art. 13(6).

4.3 The Data Act Proposal

The Data Act[140] applies to sharing and portability activities obtained from or generated by a product or service between users, data holders, and third parties. It sets out the conditions and requirements for facilitating data flows among different actors. Users of connected products or services are granted a right to access data generated by using the product from the data holder. Users can then share this data with repair or service providers (third parties). This Act bans practices undermining user rights or choices about data sharing or portability. It mandates that refusing or discontinuing data access should be as straightforward as granting it, emphasising that neither third parties nor data holders may use dark patterns in their digital interfaces. Such entities must avoid making the exercise of user rights overly difficult or manipulating users through biased, coercive, or misleading choices that compromise their autonomy or decision-making.

4.4 The AI Act

The AI Act sets out rules for development, placement on the market, and use of artificial intelligence systems ('AI systems') across the EU.

Article 5(1)(a) and (b) of the proposal details two critical provisions:[141]

> (a) AI systems must not deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm;
>
> (b) AI systems must not exploit any of the vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation, to or the effect of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm.

Article 5(1)(a) refers to subliminal techniques regarding sensory stimuli below the threshold for conscious perception. Franklin et al.[142] claim that the psychological research community has yet to draw a firm consensus about the efficacy of subliminal

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

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

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

techniques. Trappey et al.,[143] in their meta-analysis of the effectiveness of subliminal stimuli, found that it had a negligible effect size, which was not statistically significant. Accordingly, several authors[144] suggest that subliminal techniques should be replaced with a broader range of manipulation techniques.

AI-based dark patterns can consist of sophisticated, dynamic practices that employ real-time adjustments to a website/online service's UI or UX.[145] Moreover, AI-based dark patterns can also have the potential of being optimised[146] to induce specific online behaviour (micro-targeted dark patterns).

Concerning the harms caused by manipulative AI systems, it is unclear what significant harm entails, and such broad scope can encompass several types of harm (such as societal harms 'harming the democratic process, eroding the rule of law, or exacerbating inequality',[147] time, addiction, and autonomy).[148]

Article 9 of the AI Act mandates a risk assessment for AI systems, including identifying and analysing known and foreseeable risks to health, safety, and fundamental rights associated with high-risk AI systems. As this provision encompasses consumer protection and privacy fundamental rights, it can be interpreted more broadly[149] to address algorithmically driven dark patterns and algorithmic system designs that cause behavioural harm, such as addiction and loss of control (referred to here as 'darkest patterns'). Recital 70 refers to the fact that specific AI systems intended to interact with natural persons or generate content may pose specific risks of impersonation or deception, irrespective of whether they qualify as high-risk. In this line, Jarovsky[150] proposes a typology of AI-deceptive practices and gives examples thereof: AI applications or features that attempt to make people believe that (i) a particular sound, text, picture, video, or any media is genuine/authentic when it was AI-generated (false appearance); (ii) a human is interacting with them rather than an AI-based system (anthropomorphism).

[143] R. J. Trappey, and A. Woodside, *Brand choice: revealing customers' unconscious-automatic and strategic thinking processes* (Springer, 2004).

[144] R. Uuk, Manipulation and the AI Act (The Future of Life Institute, 2022); M. Franklin et al., The EU's AI Act needs to address critical manipulation methods (21 March 2023), https://oecd.ai/en/wonk/ai-act-manipulation-methods accessed 24 April 2023.

[145] Leiser, M., 'Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface' (2024) 1(1) *Journal of AI Law and Regulation*, 5–23.

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

[147] Uuk (n 146).

[148] Franklin et al. (n 143).

[149] J. 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.

[150] Dark Patterns in AI: Privacy Implications https://www.luizasnewsletter.com/p/dark-patterns-in-ai-privacy-implications accessed 8 February 2024.

Although no substantial evidence indicates the widespread use of personalised dark patterns targeting individual vulnerabilities, the growing convergence of data collection, ML, and AI techniques may alter this landscape.[151] In this line, the OECD anticipates that businesses will increasingly tailor dark patterns, enabling them to target consumers' vulnerabilities with a high granularity level and trigger mass collective harm. The EC recognises the existing evidence gap on the impact of personalised dark patterns on user decision-making. It suggests that, despite ethical challenges, future research should investigate alternative personalisation methods that employ similar personality traits without resorting to invasive data collection or exploiting vulnerabilities.[152]

Algorithmic dark patterns can be more challenging to detect and measure rather than known transactional dark patterns[153] because differences between individuals make it more challenging 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 behaviour has been manipulated. It is also challenging to reliably state that any observed differences are due to personalisation rather than A/B testing, dynamism, time, randomness, etc.

With Meta already testing AI in consumer marketing[154] and ChatGPT-4 or other AI language models[155] envisaged 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.[156]

[151] OECD (n 11); S. Mills, 'Personalised nudging' (2022) 6(1) *Behavioural Public Policy* 150–159. doi:10.1017/bpp.2020.7.

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

[153] L. Strahilevitz et al., Subcommittee Report: Privacy and Data Protection (Stigler Center Committee for the Study of Digital Platforms, 2019).

[154] 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.

[155] L. Jarosvki, Dark Patterns in AI: Privacy Implications https://www.theprivacywhisperer.com/p/dark-patterns-in-ai-privacy-implications accessed 27 April 2023.

[156] ChatGPT update tricks human into helping it bypass CAPTCHA security test *New York Post* (17 March 2023) https://nypost.com/2023/03/17/the-manipulative-way-chatgpt-gamed-the-captcha-test/ accessed 4 April 2023.

4.5 Synthesis

The EU established a regulatory patchwork for dark patterns with distinct types of protection and harm. The DSA, DMA, and Data Act proposals provide for dark pattern-specific provisions, defining the concept of dark patterns in concrete terms and containing requirements on how to design interfaces. Regarding harms, both types of consumer and data protection regimes focus on *individual harms* that dark patterns can cause. In contrast, the DSA and DMA regard *collective harms*. The DSA, because it is addressed to very large platforms and search engines, and the DMA, scoping gatekeepers, goes beyond individual harms and encompass a collective dimension of harms (or other legal consequences that dark patterns can trigger) instead. The AI Act scopes its provisions for individual, collective, and substantial harms . We claim that emergent laws have the potential to scope the darkest patterns situated at the system architecture level of digital systems. Table 3 systematises our comparative analysis of the digital design acquis within the visibility spectrum.

Table 3 Regulatory framework applicable to dark patterns with distinct types of provisions, harms, enforcement levels, and dark patterns covered within the visibility spectrum

Digital design *acquis*	**Types of provisions**	**Harms**	**Coverage**	**Authors' analysis**
DSA	Dark patterns-specific (platforms)	Collective	UI/UX	UI/UX/SA
DMA	Dark patterns-specific (gatekeepers)	Collective	UI/UX	UI/UX/SA
Data Act	Dark patterns-specific	Collective	UI/UX	UI/UX/SA
AI Act	Dark patterns-specific	Individual/ collective	Potentially SA	Potentially SA

5. Conclusion and Recommendations

This article examined the current state of enforcement decisions regarding dark patterns and the challenges of implementing the new laws to address them.

Based on our analysis of legal cases about consumer law and data protection, we found that the use of deceptive design is widespread among both large and small organisations, regardless of their business model. Also, *visible and darker* design patterns are commonly employed. Our analysis did not reveal a high prevalence of the *darkest patterns*, which may indicate either a possible gap in available evidence or enforcement capacity. The darkest dark pattern detection remains an enforcement challenge for regulators. System architecture dark patterns have the potential to impact many users negatively, yet their manipulative effects are only sometimes immediately apparent. Therefore, regulators should incorporate technical expertise from computer science and other relevant domains into their oversight and design practices.

While decisions rendered by regulators typically do not reference[157] dark patterns explicitly, they should name and denounce them to reinforce the message that they are not allowed and will be sanctioned. Regulators should clearly label dark patterns in enforcement actions to highlight their illegality and deter manipulative tactics. Publicising details of these actions (involved parties, practices, and penalties) serves dual purposes: it informs organisations of the risks and potential sanctions of adopting such practices, and it enables policymakers to understand enforcement levels and pre-emptively address similar issues. Given the rapid evolution of UI and UX design, continuous legal and regulatory updates are necessary to address emerging prohibited designs, as specific provisions in the DSA, DMA, and Data Act might soon become outdated. The EU Commission should issue clear guidelines on these prohibitions, including non-traditional interfaces like voice or virtual reality, and consider new manipulation forms like hyper-nudging or human–robot interactions under the AI Act.

[157] So far, the first and only decision explicitly mentioning dark patterns was issued by the Italian DPA against Ediscom and related to a 'visible' consent-related dark pattern type focused on the UI afforded by the controller. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014 accessed 27 April 2023.