Neutralising Deceptive Patterns: Mapping Data Protection Authorities' Roles in the Emerging Multi-Authority Landscape

Marta Beltrán[1]

[1]Agencia Española de Protección de Datos (AEPD), Madrid, Spain

Abstract

Harmful digital practices increasingly influence individuals' decisions against their best interests, often leading to diminished trust, regrettable interactions, and violations of fundamental rights. While European Data Protection Authorities (DPAs) have traditionally addressed design-based harms under the General Data Protection Regulation (GDPR), the regulatory landscape is evolving with the introduction of the Digital Services Act (DSA), the Digital Markets Act (DMA), and the AI Act. This paper examines the specific responsibilities of DPAs in addressing deceptive practices that contravene data protection principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, and data protection by design and by default. It further analyses the overlapping mandates of other supervisory bodies, such as the European Commission and national Digital Services Coordinators, which now oversee manipulative interfaces and contestability on major platforms. The analysis also identifies potential gaps in current protections, such as limited coverage for non-platform businesses and a predominant focus on economic harm. Accordingly, the paper recommends that the forthcoming Digital Fairness Act (DFA) introduce a proactive obligation of fairness by design to address the exploitation of user attention and mitigate adverse health impacts.

Keywords

Addictive patterns, Dark patterns, Data protection, Deceptive design, Harmful design, Regulation

1. Introduction

Current digital services design creates a fundamental tension with user agency, as the way choices are presented is no longer just about actual optimisation or personalisation but increasingly subverts individual autonomy [1]. Design decisions often prioritise commercial incentives, such as maximising connection time and data extraction, over the user's genuine interests and well-being [2], [3], [4]. Deceptive patterns not only cause a significant loss of agency but can also directly harm physical and mental integrity. These harmful design choices violate fundamental rights and freedoms, including the right to human dignity or to the integrity of the person, and the protection of vulnerable groups, especially children [5].

The European Union has addressed these design-based harms, first, through consumer protection regulation [6], [7]. Then, through an evolving *acquis* of digital regulations, each tackling the problem from a distinct perspective [8]. The General Data Protection Regulation (GDPR, [9]) provides the foundation, enforcing different principles and requirements to safeguard the fundamental rights of data subjects when personal data is processed. Complementing this, the Digital Services Act (DSA, [10]) explicitly bans manipulative tactics and dark patterns on online platform interfaces to ensure a safer digital environment. The Digital Markets Act (DMA, [11]) targets the systemic power of "gatekeepers", prohibiting them from using behavioural techniques or interface designs to circumvent their obligations and undermine market contestability. Finally, the AI Act [12] prohibits the use of AI systems that deploy subliminal or purposefully manipulative techniques intended to distort behaviour and cause significant harm.

Bridge Over Troubled Water: Aligning Commercial Incentives With Ethical Design Practice To Combat Deceptive Patterns. Workshop at the 2026 CHI Conference on Human Factors in Computing Systems (CHI EA '26), April 13–17, 2026, Barcelona, Spain.

mbeltran@aepd.es (M. Beltrán)

0000-0002-1689-7479 (M. Beltrán)

This paper contributes to the workshop by analysing the specific role of Data Protection Authorities (DPAs) in applying GDPR principles, such as lawfulness, fairness, transparency, purpose limitation, data minimization, and data protection by design, to neutralise harmful design. It also examines coordination challenges between DPAs and other supervisory bodies under the new DSA, DMA, and AI Act frameworks. Finally, the paper identifies critical scope and harm gaps, such as the exclusion of non-platform businesses from certain protections. It proposes a framework for the future Digital Fairness Act (DFA) based on a positive duty of "fairness by design", providing specific recommendations for regulatory authorities and HCI (Human-Computer Interfaces) researchers.

The rest of this paper is structured as follows. Section 2 examines the relationship between data protection and safeguards against deceptive design. Section 3 analyses the role of European regulations, distinct from those addressing data protection, in providing such safeguards and highlights the necessity for coordination and synergies. Section 4 identifies gaps in existing regulations, justifying the need for the new Digital Fairness Act. Section 5 offers recommendations for regulatory authorities and researchers in light of this context. Finally, Section 6 summarises our main conclusions.

2. The Role of Data Protection Authorities in Fighting Design Harms

European DPAs enforce the GDPR as a principal mechanism for addressing and sanctioning design choices that violate data subjects' rights and freedoms. They can do this in two ways, either through soft law or through hard law.

2.1. EU DPA's soft law: guidelines, reports and scientific research

The European Data Protection Board (EDPB) has issued Guidelines 03/2022, targeting deceptive design patterns in social media interfaces [13]. The EDPB defines dark patterns as interface and user experience (UX) choices that lead users to unintended, unwilling, and potentially harmful decisions regarding personal data, and maps them to specific GDPR provisions. The guidelines state that DPAs are responsible for sanctioning dark patterns that breach GDPR and identify affected principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, and data protection by design and default.

These guidelines also provide a standardised typology of tactics used to influence users into making unintended and potentially harmful decisions about their personal data. The EDPB categorises these patterns into six functional groups: overloading, skipping, stirring, hindering, fickle and left in the dark. Finally, these guidelines offer best practices to avoid undesirable yet still formally legal designs, positioning DPAs as standard-setters for UX in social media and similar interfaces.

The French DPA, CNIL, has developed a broader "Données & Design" line of work and has published guidelines and blog analyses on misleading design (dark patterns) in interfaces, including work on cookie consent designs and a conceptual "grille de lecture" for regulating deceptive design practices [14]. CNIL's work on dark patterns in cookie banners frames misleading consent journeys as a transparency and consent problem.

The Spanish DPA, AEPD, has clarified the link between personal data processing and addictive patterns [15]. The AEPD defines these patterns as design features intended to make users spend more time or show a higher degree of commitment than is healthy or expected. Relying on a systematic review of scientific evidence, the AEPD developed the FoSIP framework [16], which classifies addictive approaches into four high-level strategies: Forced Action (such as endless scrolling or streaming), Social Engineering (exploiting Fear Of Missing Out or social proof, for example), Interface Interference (such as aesthetic manipulation), and Persistence (using micro-interruptions or nagging, for example).

A key contribution of the AEPD is framing addictive design as a fundamental rights issue, specifically citing a violation of the right to physical and mental integrity under Article 3 of the EU Charter of Fundamental Rights [17]. The AEPD work also identifies affected principles and requirements: lawfulness, fairness, transparency, purpose limitation, data minimisation, accountability, data protection by design and default, processing of special categories of personal data, and automated individual decision-making, including profiling. Additionally, the AEPD argues that because prolonged exposure

to these patterns can lead to sleep disturbances, anxiety, and behavioural modification (high-risk data processing), controllers are obligated to perform a Data Protection Impact Assessment (DPIA). The AEPD asserts that such processing would rarely pass a proportionality test, making many addictive designs inherently non-compliant with the GDPR.

2.2. EU DPA's hard law: sanctions and corrective orders

Under GDPR and national law, DPAs deploy administrative fines, orders to comply/cease processing, and, in some contexts, temporary bans or restrictions, explicitly when deceptive practices undermine the validity of consent or breach fairness and transparency.

The Italian DPA, Garante, imposed a 300.000 euros fine on a digital marketing services company for the use of dark patterns in obtaining marketing consent, finding that interfaces which made the consent button prominent while relegating "continue without accepting" to small, less visible text outside the main banner constituted manipulative design incompatible with freely given consent under GDPR [18].

CNIL has issued formal notices to multiple website publishers whose cookie banners used dark patterns (unequal button visibility, misleading wording, cumbersome rejection paths), ordering them to comply within one month or face sanctions for violations of Article 82 of the French Data Protection Act [19]. CNIL's cookie recommendations explicitly discourage "unequal path to decline" designs where refusal requires extra steps (e.g., hidden under "customise my choices"). This pattern has also been considered a regulatory violation.

Spain's AEPD has opened sanctioning procedures and imposed fines where website owners used dark patterns around cookies and consent, such as overloading users with long lists of providers without a single reject-all button and default-ticked boxes for many third-party providers, linking these patterns to breaches of fairness, transparency, and the duty to inform (Article 13 GDPR). In its first resolution explicitly addressing dark patterns online [20], the AEPD qualified practices such as overloading and skipping (e.g., no single button to object to processing by 130 providers, pre-ticked boxes) as infringements of Article 5(1)(a) GDPR and used the scope/purpose of processing as an aggravating factor when calculating the sanction.

The Norwegian DPA has taken enforcement action against several websites that use tracking pixels in sensitive contexts, such as health and domestic violence support. It identified textbook dark patterns in consent banners, including bright "accept all" buttons and barely visible "necessary only" options, and stressed that such manipulation is incompatible with genuine consent, especially for vulnerable populations [21]. In these Norwegian cases, the authority highlighted misrepresentation (promises of anonymity contradicted by actual tracking) and the emotional and situational vulnerability of users. It concluded that third-party tracking combined with manipulative design was largely inappropriate when serving children and people in crisis.

Finally, it is worth mentioning the Irish DPA's 345 million euros TikTok fine, in which dark patterns such as preselected public profiles for children and visually dominant "Post Now" prompts violated fairness by nudging minors into privacy-invasive defaults and exploiting their developmental vulnerabilities [22].

3. The Emerging Multi-Authority Enforcement Landscape

Both the EDPB's guidance on deceptive patterns in social media and the AEPD's report on addictive patterns highlight regulatory overlaps and advocate for structured cooperation to harmonise actions against these deceptive practices. This approach highlights that such patterns often have simultaneous implications for data protection, platform regulation, competition and markets.

3.1. Digital Services Act (DSA)

The DSA ([10]) represents a shift from case-by-case enforcement to a structural regulatory model that explicitly bans dark patterns on online interfaces. Under Article 25, providers of online platforms are

prohibited from designing, organising, or operating their interfaces in a way that deceives, manipulates, or otherwise materially distorts users' ability to make free and informed decisions. The DSA characterises these patterns as practices that impair user autonomy, whether intentionally or through their effects. Regulators are therefore required to demonstrate only the measurable impact on users, rather than proving the designers' deceptive intent.

Although the DSA does not offer a single legal definition of addictive patterns, its framework is structured to address such practices through risk-mitigation obligations. Recitals 81 and 83 explicitly acknowledge that online interface designs can foster behavioural addictions, especially among minors. For Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), Articles 34 and 35 extend obligations to address systemic risks associated with the design, operation, or use of these services. These provisions explicitly require risk assessments and mitigation measures when interface or recommender system design contributes to mental harm, behavioural addiction, or non-consensual changes to users' mental states.

Article 35(1) provides examples of mitigation measures directly related to design, such as modifications to interfaces, recommendation algorithms, advertising delivery, and nudging strategies. These measures aim to reduce users' exposure to deceptive and manipulative practices. Furthermore, the DSA requires VLOPs to offer at least one recommender system that does not rely on profiling (Article 38). This enables users to select non-personalised feeds, such as chronological order, which can help prevent rabbit-hole effects and addictive content loops.

Recent work interprets Articles 34 and 35 as requiring VLOPs to address mental health harms, including addiction, attentional exhaustion, and non-consensual mood manipulation, as systemic risks arising from design choices such as infinite scroll, variable-reward notifications, or friction-heavy opt-outs [23]. According to this interpretation, failing to acknowledge credible empirical evidence of mental harms in risk assessments, or to link these harms to choice architecture and recommender design, may constitute a violation of Articles 34 and 35, regardless of whether specific dark patterns are addressed under Article 25.

Enforcement of the DSA is a shared responsibility between national and EU-level authorities. Each Member State designates an independent Digital Service Coordinator (DSC) to supervise and enforce compliance within its territory. DSCs serve as the primary point of contact for citizens to file complaints about DSA violations. The European Commission has sole supervisory power over VLOPs and VLOSEs due to the significant systemic risks these platforms pose. Finally, the European Board for Digital Services acts as an independent advisory group to coordinate the DSCs and the Commission and ensure consistent application of the regulation.

Under Article 25(3), the Commission is authorised to issue guidelines on specific dark patterns and their appropriate addressing. This allows for a more flexible, evolving response to emerging deceptive tactics without requiring new legislation. So far, no document has been published in this line. However, the Commission maintains ongoing contact with large platforms to support and supervise compliance before formal investigations become necessary.

The Commission has already employed hard law enforcement tools in several notable cases. In December 2025, it imposed a non-compliance fine of 120 million euros on X (formerly Twitter), specifically citing dark patterns and transparency failures [24]. In 2024, the Commission initiated an investigation into the TikTok "Rewards" program due to concerns about its potentially addictive design for children, resulting in the program's withdrawal in response to regulatory pressure [25]. Ongoing investigations are examining potentially addictive behaviours in children, and rabbit-hole effects caused by endless content paths on both Temu [26] and Meta [27]. Finally, the European Commission has recently preliminarily found TikTok in breach of the DSA for its addictive design [28].

3.2. Digital Markets Act (DMA)

The DMA ([11]) aims to promote contestability and fairness in digital markets by regulating "gatekeepers", which are large platforms providing core services such as search engines, social networks, and app stores. In contrast to traditional antitrust law, the DMA introduces specific rules to safeguard end users'

freedom of choice and to maintain a level playing field for business users. A fundamental principle of the DMA is that compliance must be substantive; the European Commission has emphasised that nominal compliance is inadequate if technical or psychological barriers persist.

The prohibition on circumvention under Article 13(4) of the DMA is the primary mechanism to address design-based harms. This provision explicitly prohibits gatekeepers from employing behavioural techniques or interface designs that undermine effective compliance with their obligations. It encompasses designs that, although formally compliant, violate the intent of the law by subverting user autonomy or choice. For example, a key focus of this article is the use of "scare screens", which are prompts that leverage warnings about security or quality to instil fear and deter users from exercising their rights, such as switching to alternative payment systems or using other app stores.

The DMA also addresses the data-driven basis of deceptive design. Article 5(2) prohibits gatekeepers from combining personal data across different services without obtaining explicit and specific consent. Gatekeepers are required to offer users a less personalised yet equivalent alternative that does not compromise service quality. Additionally, Article 15 mandates that gatekeepers provide an independently audited description of their profiling techniques, which the Commission forwards to the EDPB to facilitate regulatory coordination.

The European Commission serves as the sole enforcer of the DMA. To support this mandate, the Commission is assisted by a High-Level Group comprising representatives from different authorities and organisations. The Commission has soft law powers to promote compliance before imposing fines. Pursuant to Article 47, the Commission may issue guidelines on any aspect of the Regulation to provide legal certainty for gatekeepers. The European Commission, in collaboration with the EDPB, has issued joint guidelines addressing the relationship between the DMA and the GDPR. These draft guidelines, endorsed in October 2025, clarify compliance requirements for gatekeepers regarding data access, portability, consent, and anonymisation, while ensuring alignment between DMA obligations and data protection rules. A public consultation on these guidelines concluded in December 2025, with final adoption anticipated in 2026.

The Commission is also empowered to initiate market investigations to revise gatekeeper obligations, ensuring that the DMA remains effective against emerging harmful design patterns and manipulative practices in the digital sector. In April 2025, the Commission issued its first significant non-compliance decisions. Meta was fined 200 million euros for its "pay or consent" model, which the Commission found compelled users to choose between two options without providing a genuinely less personalised free alternative. Although this model has been criticised for nudging users toward data consent and raising concerns about dark patterns, the ruling primarily addressed the equivalence of available choices. Alphabet is currently under investigation for potentially using interface designs that favour its own search services over competitors'.

3.3. AI Act

Artificial Intelligence (AI) has become essential for deploying deceptive patterns, serving as the technological foundation that enables manipulation through real-time, highly personalised strategies. AI systems rely on their inference capabilities to build models from data, generating predictions, content, and recommendations that shape users' virtual environments and autonomy. For instance, generative AI and Large Language Models (LLMs) can produce personalised, emotionally targeted deceptive prompts in real time, exploiting specific psychological vulnerabilities. AI-driven profiling can identify and leverage weaknesses related to age, disability, or socio-economic status to influence behaviour. Algorithmic recommendations represent a particularly potent addictive design pattern, amplifying other manipulative techniques and guiding users through continuous content streams that foster harmful behaviours.

As deceptive patterns become increasingly automated and autonomous due to AI, the AI Act serves as an essential regulatory instrument to address harmful design [12]. The Act adopts a risk-based framework that imposes strict prohibitions on certain AI-enabled manipulative practices. Article 5(1)(a) of the Regulation forbids the marketing or use of AI systems that employ subliminal techniques beyond

conscious awareness or intentionally manipulative or deceptive methods designed to distort behaviour. A practice is prohibited if it significantly impairs a user's capacity to make informed decisions, resulting in choices they would not otherwise make and causing, or being likely to cause, significant harm.

Additionally, Article 5(1)(b) prohibits AI systems that exploit the vulnerabilities of specific groups, including those defined by age, disability, or socio-economic status, to distort behaviour and cause significant harm. Although the Act does not explicitly reference "dark patterns" or "addictive patterns", these provisions are intended to address design-driven manipulations that constitute unacceptable risk.

Beyond explicit prohibitions, Article 13 requires that high-risk AI systems be designed to ensure sufficient transparency, enabling deployers to interpret outputs and use the system appropriately. Article 14 further mandates human oversight, requiring that systems be designed so that natural persons can effectively monitor their functioning and interrupt the system via a "stop" button. For systems that interact directly with natural persons, Article 50 introduces transparency obligations, requiring that users be informed they are interacting with an AI, unless this is obvious from the context. Furthermore, providers of AI that generate synthetic content (e.g., deep fakes) must ensure outputs are marked in a machine-readable format and are detectable as artificially generated.

The AI Act establishes a governance framework to oversee its principles and requirements, composed of the AI Office within the European Commission (supported by a Scientific Panel of independent experts), competent authorities appointed at each Member State and the European Artificial Intelligence Board.

The Commission is mandated by Article 96 to develop guidelines on the practical implementation of the AI Act. In addition, Article 4 imposes an obligation on providers and deployers to ensure that their staff possess sufficient AI literacy, taking into account the context of AI use and the affected groups. These measures, along with codes of practice (for example, the GPAI -General Purpose AI- Code of Practice to help providers comply with transparency and safety obligations) and regulatory sandboxes (Member States must establish at least one to provide a controlled environment for testing innovative developments), should help to bridge the gap between legal principles and requirements and technical implementation.

Compliance is reinforced by some of the highest financial penalties in EU digital law, as stipulated in Article 99. The sanction regime is not yet operational. Enforcement of penalties is scheduled to commence on August 2 2026, at both national and EU levels, coinciding with the implementation of high-risk AI rules.

3.4. The Need for Synergy

A single design choice can frequently violate multiple regulations simultaneously, necessitating a coordinated response based on clear, horizontal standards rather than case-by-case assessments. For example:

- Pre-ticked consent boxes: An interface design where an option, such as agreeing to the processing of personal data or accepting tracking cookies, is selected by default before the user has made a choice may infringe the GDPR (invalid consent under Article 7, fails transparency, etc.), the DSA (manipulative interface limiting free choice under Article 25), the DMA (circumvents steering rules for gatekeepers under Article 13) and the AI Act if AI-powered (prohibited practice under Article 5, for example, if exploiting specific vulnerabilities).
- Fake scarcity timer: An interface design that creates artificial pressure by falsely claiming that an offer or deal is strictly time-limited to distort a user's rational decision-making, manufacturing a sense of panic or a "fear of missing out". This design may infringe the GDPR (different principles under Article 5), the DSA (systemic risk via deception, Article 34 if implemented by a VLOP), the DMA (undermining user decisions for platform gain), and the AI Act (subliminal manipulation if AI-generated, prohibited under Article 5).
- Confirmshaming: An interface that uses emotive language or shaming to pressure a user into making a specific choice, framing the alternative (often the one that protects the user's privacy or

financial interests) as a detrimental, socially unacceptable, or foolish decision. For example, "Hey, a lone wolf, are you? But sharing and connecting with others help make the world a better place!". This pattern may infringe the GDPR (coerced consent under Article 7, data protection by design and by default under Article 25, etc.), the DSA (emotional manipulation impairing autonomy), the DMA (gatekeeper nudge against user interest), and the AI Act (behavioural distortion via AI profiling).

To address these challenges, policymakers have established the High-Level Group for the DMA, a specialised body comprising representatives from the EDPB, the European Data Protection Supervisor (EDPS), the European Competition Network, the Consumer Protection Cooperation Network, the Body of European Regulators for Electronic Communications (BEREC), and the European Regulators Group for Audiovisual Media Services (ERGA). This group provides the European Commission with multidisciplinary expertise to ensure a consistent regulatory approach across various instruments. Effective enforcement from 2026 onward will increasingly depend on such cooperation mechanisms, enabling supranational and national authorities to coordinate investigations and share technical evidence related to deceptive choice architecture, for example, through joint case referrals or shared audits.

Synergy is also being built through soft law tools, such as joint guidance, codes of conduct, or regulation interplay analysis. Policymakers should prioritise the creation of joint guidance between the AI Office, the European Board for Digital Services, and the EDPB to provide clear, cross-regulatory taxonomies of prohibited design practices, for example.

This layered approach allows regulators to progressively build a specific doctrine on deceptive patterns while aligning it with adjacent fields (GDPR, DSA, DMA, AI Act, consumer protection regulation), gradually transforming design-level choices into accountable questions on digital fairness and fundamental rights protection. Looking forward, the Digital Fairness Act (DFA) is expected to fill critical gaps by introducing a positive duty of "fairness by design", which would apply to commercial practices that fall outside the current scope of the GDPR (processing-centric) or of platform-, market- or implementation-specific laws [29].

4. Identifying Regulatory Gaps for the Future Digital Fairness Act (DFA)

The preceding analysis demonstrates that the current regulatory framework, although comprehensive, continues to exhibit gaps in scope and harm that the recently proposed DFA ([29]) should address.

Scope gaps arise when existing regulations do not address particular business sectors, technical implementations, or legal triggers.

The GDPR establishes a baseline for the protection of fundamental rights and freedoms, but its scope is limited to situations involving the processing of personal data. The DFA should be structured to address harmful practices even when personal data processing does not occur.

Although the DSA explicitly prohibits dark patterns, its most stringent provisions apply primarily to online platforms, especially those classified as "Very Large". In contrast, the DFA is expected to cover a broader range of digital businesses, including e-commerce sites, video games, and mobile applications that may not fall within the DSA's definition of a platform.

The DMA is based on broad principles regarding user autonomy and choice, but it does not include specific prohibitions tailored to digital interface design. The DFA aims to introduce a "fairness by design" obligation and a detailed list of prohibited practices to enhance legal certainty.

The AI Act prohibits manipulative techniques only when they are likely to result in "significant harm". The DFA should seek to address deceptive AI-driven patterns that, while not meeting this high-harm threshold, nonetheless undermine consumer autonomy or integrity.

On the other hand, harm gaps denote forms of user injury, frequently non-monetary, that are insufficiently recognised or protected by current regulatory frameworks.

Existing law frequently associates unfairness with a "transactional decision" to purchase a product or use a service. The DFA should broaden this definition to encompass situations in which consumers provide data and time in exchange for "free" services. The DFA should further expand the traditional perspective by recognising time loss and attention capture as quantifiable harms, and treating user attention as a monetisable asset that platforms often extract through deceptive design.

Current regulations primarily address financial harms or explicit and direct violations of rights and freedoms. The DFA should target adverse health effects resulting from addictive design patterns, including sleep disturbances and anxiety. Additionally, existing laws often presume that users are rational economic actors and provide specific protection only for vulnerable groups, such as children. The DFA should recognise universal vulnerability, as modern deceptive patterns based on highly personalised strategies are sufficiently sophisticated to exploit the psychological weaknesses of any individual, thereby justifying a horizontal fairness standard.

5. Recommendations to Build Transdisciplinary Bridges

5.1. For regulatory and enforcement authorities

The existing regulatory framework already provides operational mechanisms to address deceptive design practices, and the new regulation can strengthen them if it covers the gaps already mentioned.

Data Protection Impact Assessments (DPIAs), as outlined in Article 35 of the GDPR, can serve as a procedural tool for DPAs to evaluate design choices before implementation. When personal data processing is involved, DPAs may use prior consultation to require design modifications before deployment, particularly when deceptive patterns are integrated into the core engagement mechanisms of digital products and services. Additionally, DPAs could incorporate UX reviews into routine audits, assessing processes such as consent flows, account deletion, and settings (including children's default settings), rather than focusing solely on static privacy policies. Increasingly, mandates to implement specific design modifications, such as button symmetry, default protective settings, and simplified withdrawal processes, are becoming central methods by which enforcement authorities influence interface design.

Enhanced formal and structural cooperation among regulatory authorities is necessary to leverage present and future regulatory complementarity fully. Regulatory authorities should prioritise coordinated enforcement actions, including the publication of joint guidance (e.g., definitions, taxonomies, and acceptable/prohibited practices) and the creation of databases cataloguing decisions on deceptive practices to inform evidence-based guidance for companies on choice architecture. For example, authorities may collaborate to mandate non-personalised options by default for content feeds and recommender systems. In light of the increasing sophistication of AI-based deceptive patterns, authorities could establish a unified approach to accountability, shifting the burden of proof to providers and deployers. If a company cannot demonstrate that its service design is fair, the design should be presumed unfair.

5.2. For the Human-Computer Interaction research community

Researchers in HCI provide scientific evidence that enables regulatory and enforcement authorities to address deceptive design practices. They provide frameworks for regulators to identify, categorise, and assess harmful design practices by explicitly distinguishing between deceptive, manipulative, and addictive attributes.

Building on these frameworks, a significant contribution of HCI is its capacity to measure and quantify harms that regulation has historically struggled to address. HCI researchers can provide empirical evidence on how specific design choices lead to time loss, psychological manipulation, and adverse health outcomes. For children, HCI research is crucial in identifying emerging risks, including those associated with advergames, non-transparent influencer advertising, the integration of advertising models into AI systems and subscription traps that exploit their inexperience.

Expanding further, HCI studies can also demonstrate how hyper-personalised algorithmic recommendations and profiling methods contribute to the implementation of addictive strategies. Researchers can assist authorities in understanding how these systems exploit individual user weaknesses or vulnerabilities to influence decisions that users might not otherwise make.

Beyond identifying harmful practices, HCI researchers can contribute to establishing benchmarks for fair design by studying default settings, such as providing evidence for the effectiveness of non-personalised options in content feeds and recommendations. They can also help propose and evaluate design alternatives. For example, transparency mechanisms that provide users with clear information and intervention tools, including technical safeguards such as stop buttons or neutral interface formats, to protect user autonomy and re-route user experiences.

Taken together, these activities highlight that HCI experts can collaborate with different authorities, providing technically qualified alerts and the multidisciplinary expertise needed to ensure consistent enforcement of existing regulations.

6. Conclusions

The advancement of ethical design requires a harmonised regulatory framework in which the forthcoming Digital Fairness Act (DFA) operates in full complementarity with the existing EU digital *acquis*. Instruments such as the GDPR, the DSA, the DMA, and the AI Act have established important limitations and prohibitions to address deceptive interfaces and harmful design practices. Nevertheless, these regulations leave significant gaps regarding legal triggers in cases where personal data processing is not involved, businesses that are not online platforms, and harms that are neither consumer-traditional nor meet the high-risk thresholds defined by the AI Act. The DFA should address these deficiencies by introducing a horizontal fairness-by-design obligation and integrating consumer protection throughout the digital product development lifecycle.

This regulatory evolution enables authorities to address the complexities of the attention economy, in which consumer harm includes not only financial loss but also time loss and adverse health outcomes. The effectiveness of this digital framework depends on robust, multidisciplinary enforcement, based on formalised cooperation mechanisms between data protection authorities and other regulatory bodies. Successful enforcement requires policymakers to move beyond broad, principle-based rules and to adopt specific, evidence-based prohibitions regarding design patterns. By relying on scientific evidence, both existing regulations and the forthcoming DFA can offer the technical clarity required to counter deceptive and harmful design.

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly in order to: Grammar and spelling check, Paraphrase and reword. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] S. Ahuja, J. Kumar, Conceptualizations of user autonomy within the normative evaluation of dark patterns, Ethics and Information Technology 24 (2022) 52. doi:10.1007/s10676-022-09672-9.

[2] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, A. L. Toombs, The dark (patterns) side of UX design, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, p. 1–14. doi:10.1145/3173574.3174108.

[3] A. Mathur, M. Kshirsagar, J. Mayer, What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods, in: Proceedings of the 2021 CHI conference on Human Factors in Computing Systems, 2021, pp. 1–18.

[4] J. Luguri, L. J. Strahilevitz, Shining a light on dark patterns, Journal of Legal Analysis 13 (2021) 43–109. doi:10.1093/jla/laaa006.
[5] M. Brenncke, A theory of exploitation for consumer law: Online choice architectures, dark patterns, and autonomy violations, Journal of Consumer Policy 47 (2024) 127–164. doi:10.1007/s10603-023-09554-7.
[6] W.-T. Yang, M. Leiser, Illuminating manipulative design: From "dark patterns" to information asymmetry and the repression of free choice under the unfair commercial practices directive, Loyola Consumer Law Review 34 (2022) 484. URL: https://lawecommons.luc.edu/lclr/vol34/iss3/6.
[7] S. De Conca, The present looks nothing like the Jetsons: Deceptive design in virtual assistants and the protection of the rights of users, Computer Law & Security Review 51 (2023) 105866. doi:10.1016/j.clsr.2023.105866.
[8] M. Leiser, C. Santos, Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface, European Journal of Law and Technology 15 (2024). URL: https://ejlt.org/index.php/ejlt/article/view/990/1084.
[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[10] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 october 2022 on a single market for digital services and amending directive 2000/31/ec (Digital Services Act), 2022. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.
[11] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 september 2022 on contestable and fair markets in the digital sector and amending directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng.
[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 june 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC) no 300/2008, (EU) no 167/2013, (EU) no 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
[13] European Data Protection Board, EDPB guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them, 2022. URL: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.
[14] CNIL, Data & design, 2022. URL: https://design.cnil.fr/en/concepts/.
[15] AEPD, Addictive patterns in the processing of personal data: Implications for data protection, 2024. URL: https://www.aepd.es/guides/addictive-patterns-in-processing-of-personal-data.pdf.
[16] M. Beltrán, Defining, classifying and identifying addictive patterns in digital products, IEEE Transactions on Technology and Society 6 (2025) 314–323. doi:10.1109/TTS.2025.3564840.
[17] AEPD, Addictive patterns and the right to the integrity of the person, 2024. URL: https://www.aepd.es/en/guides/addictive-patterns-and-the-right-to-integrity.pdf.
[18] Garante per la protezione dei dati personali, Provvedimento prescrittivo e sanzionatorio nei confronti di ediscom s.p.a. - 23 febbraio 2023 [9870014], 2023. URL: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870014.
[19] CNIL, Dark patterns in cookie banners: CNIL issues formal notice to website publishers, 2024. URL: https://www.cnil.fr/en/dark-patterns-cookie-banners-cnil-issues-formal-notice-website-publishers.
[20] AEPD, Resolucion de procedimiento sancionador exp202211953 (ps/00080/2023), 2023. URL: https://www.aepd.es/documento/ps-00080-2023.pdf.
[21] Datatilsynet, Ulovlig deling av personopplysninger gjennom sporingspiksler hos seks nettsteder, 2025. URL: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2025/ulovlig-deling-av-personopplysninger-gjennom-sporingspiksler-hos-seks-nettsteder/.
[22] Data Protection Commission, In the matter of TikTok technology limited, 2023. URL:

https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf.
[23] P. Pałka, E. Ilczuk, Social media and mental harms under the Digital Services Act, Internet Policy Review 15 (2026). doi:10.14763/2026.1.2056.
[24] European Commission, Commission fines X €120 million under the Digital Services Act, 2025. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934.
[25] European Commission, TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act, 2025. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161.
[26] European Commission, Commission opens formal proceedings against Temu under the Digital Services Act, 2025. URL: https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-temu-under-digital-services-act.
[27] European Commission, Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram, 2025. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664.
[28] European Commission, Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act, 2026. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312.
[29] European Parliament, Digital Fairness Act: Legislative train schedule, 2025. URL: https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-digital-fairness-act.