Feedback to the European Commission's Call for Evidence for an Impact Assessment the Digital Fairness Act

Who are we?

The Working Group on Gaming and Regulation was launched in September 2024 with the aim of providing informed and constructive input on regulation affecting the global gaming industry. The group brings together representatives of the gaming industry, civil society researchers, and regulators on a weekly basis to discuss regulatory gaps, challenges, and opportunities. Its multi-stakeholder composition is designed to facilitate dialogue across sectors and interest groups sometimes assumed to be in opposition. United by the belief that regulation must play a role in fostering a healthy and responsible gaming ecosystem, the working group members engage in weekly discussions to achieve consensus on pragmatic regulatory proposals and critiques. In recognition of its potential to provide valuable feedback to regulators worldwide, the working group became an official observer to the Global Online Safety Regulators Network (GOSRN) in November 2024.

Members of the Working Group who contributed to this feedback (in alphabetical order):

- Martin Sas, Centre for IT and IP law (CiTiP) of KU Leuven
- Noémie Krack, Centre for IT and IP law (CiTiP) of KU Leuven
- Ingrida Milkaite, VUB & Ghent University
- Mariana Olaizola Rosenblat, NYU Stern Center for Business and Human Rights
- Samantha Bradshaw, American University School of International Service

Contextualisation: digital fairness in the gaming sector

The Commission's Fitness Check of EU Consumer Law on Digital Fairness has highlighted important gaps in consumer protection, particularly with respect to harms caused by dark patterns, "addictive" design features, and unfair personalisation practices such as targeted advertising and exploitative data monetisation. **These risks are especially acute in digital gaming,** where players are routinely exposed to manipulative and exploitative design strategies (Van Rooij et al., 2021).

With the sector now dominated by free-to-play models, providers depend on revenues from **in-game purchases and advertising** (Alha, 2020; Ekambaranathan, et al., 2021). This creates strong incentives to deploy **dark patterns** or other **manipulative and deceptive techniques** to prolong playtime, maximise exposure to advertising and personal data sharing, and intensify pressure to spend (Zagal et al., 2013 ; King et al., 2019 ; Petrovskaya & Zendle, 2021). The

collection of players' (engagement and personal) data and the use of game telemetry[1] further enables the collection of detailed behavioural data (Sifa et al., 2018), facilitating **highly personalised marketing** strategies that raise both **privacy concerns** and heightened risks of **exploiting player vulnerabilities** (Newman et al., 2014; Kroger et al., 2023). The imbalance between providers' extensive behavioural insights and players' reasonable expectations of a safe, entertainment-oriented environment exacerbates this vulnerability (Sax & Ausloos, 2021; Dechant et al., 2023).

Previous enforcement actions by national authorities (ACM, 2023; CPC-N, 2025) have shown that **certain unfair practices in digital games** – such as direct exhortations to children, misleading scarcity indicators, time-limited offers, and lack of transparency about commercial content – **can be addressed under the Unfair Commercial Practices Directive (UCPD)**. However, significant difficulties remain in addressing the full range of consumer harms that may arise from the design of digital games.

Against this backdrop, the EU Consumer Agenda 2025–2030 and the proposed Digital Fairness Act offer timely opportunities to strengthen consumer protection in digital gaming. We, therefore, welcome these initiatives but emphasize that they should **focus on updating and clarifying existing rules, closing identified gaps, and ensuring consistent and effective enforcement across Member States, rather than adding further layers of regulatory complexity.** These recommendations have already been partially formulated in our previous feedback to the EU Consumer Agenda 2025-2030 and will be further specified below with regard to the Digital Fairness Act.

Our recommendations for the upcoming Digital Fairness Act (DFA)

Providing clarity and avoiding fragmentation

Concerning dark patterns and other manipulative and deceptive practices, **the current legal framework is already complex and highly fragmented.** The EU Unfair Commercial Practices Directive (UCPD) and the General Data Protection Regulation (GDPR) provide broad horizontal coverage to all Business-to-Consumer (B2C) relationships where personal data are processed, but do not explicitly address dark patterns as such, creating difficulties for the detection, evaluation and sanction of infringements. More recent instruments, such as the Digital Services Act (DSA), Digital Markets Act (DMA), Data Act (DA), and Artificial Intelligence Act (AIA), provide explicit prohibitions of certain types of dark patterns but are restricted to specific actors or situations due to limitations in their scope of application. The DMA deliberately limits its application to the biggest actors (e.g., "core platform services"),[2] leaving the vast majority of online services outside its reach. The DA targets dark patterns only to the extent that they interfere with the user's ability to access and share data generated by connected products and

[1] Game telemetry is the term we use to denote any source of data obtained over distance which pertains to game development or game research. There are many popular applications of telemetry in games, including remote monitoring and analysis of game servers, mobile devices, user behavior and production (Drachen, 2012).
[2] See the definition laid down in Art. 2(2) of the DMA.

related services.[3] The AI Act captures only a narrow subset of dark patterns, namely those embedded in AI systems that exploit vulnerabilities or use subliminal techniques to materially distort user behaviour and cause significant harm.[4] As for the DSA, the explicit prohibition of deceptive and manipulative designs laid down in Art. 25 only applies to "online platforms"[5] and is itself restricted to situations which are not yet covered by the UCPD or the GDPR.[6]

Instead of creating more complexity by adding an extra layer of regulation on dark patterns, the DFA should harmonise these prohibitions and **clarify how the UCPD's prohibitions apply to specific use of dark patterns across digital environments**, for example, via **new prohibition under Annex I** of that Directive. The list of prohibited practices should adopt a "technology-specific" approach, accounting for the diverse ways that unfair practices manifest themselves in specific contexts and through specific technologies. While technology neutrality brings some flexibility in adapting to new forms of unfair practices stemming from rapid and ever-changing technological developments, it also creates uncertainty when assessing whether a particular interface can be deemed compliant or not. Without further specification on what is prohibited or prescribed, it can be hard to distinguish between acceptable and inacceptable designs. While the broad and abstract prohibitions under Art. 5 UCPD should be maintained to allow for flexibility, Annex I could prohibit specific manifestations of dark patterns identified as harmful to consumers (see, for example, the dark patterns identified in the ontology developed by Gray et al., 2024). **Clearer technology-specific prohibitions would both ensure legal clarity for business and facilitate the detection and evaluation of legal infringements, therefore, contributing to better enforcement.** In that regard, the Key Principles on In-game Virtual Currencies issued by the CPC Network in March 2025 constitute valuable examples in the gaming sector of technology-specific prohibitions and prescriptions which could be made legally binding.

Finally, to remain up-to-date, the Annex I's list of prohibited practices should be periodically reviewed and amended using faster mechanisms like delegated or implementing acts, allowing for more agile responses to technological changes and involving stakeholders through co-regulation, rather than relying solely on lengthy legislative procedures.

Concerning unfair and exploitative personalisation. Scholars argue that the widespread personalisation of commercial practices creates information asymmetries and power imbalances which place every user in a position of vulnerability (Helberger, 2022; Drazewski, 2022). This new form of "digital" vulnerability goes beyond traditional group-based vulnerabilities (i.e., vulnerabilities based on mental or physical infirmity, age or credulity) as it plays a structural role in the online environment (Riefa, 2022). In this context, profiling techniques can be used to place consumers in a vulnerable position as these techniques, by predicting and influencing the consumer's behaviour, can undermine their decisional autonomy (Duivenvoorde, 2023; Zac et al., 2025). Given their adverse impact on individuals, such practices can be seen as incompatible with the principle of fairness underlying both the GDPR and the UCPD - especially

[3] See Recital 38(1), Arts. 4(3)(a)-(9)(a), 5(12)(a), 17(5), and 38(1) of the DA.
[4] Art. 5(1)(a) and (b) of the AIA.
[5] See the definition laid down in Art. 3(i) of the DSA.
[6] Pursuant to 2nd paragraph of Art. 25.

when it concerns children who are entitled to specific protection in relation to the processing personal data under recital 38 GDPR (Leijten & van der Hof, 2025, van der Hof et al., 2020). To address harmful personalisation, **the DFA could introduce specific prohibitions in the UCPD's Annex I**; such as presenting **targeted advertising to consumers based on the processing of their special categories of personal data** listed in Art. 9 GDPR, or presenting **targeted advertising to minors**. While these practices are already explicitly prohibited under Art.s 26(3) and 28(2) of the DSA, such prohibitions only concern targeted ads when they are presented via the interfaces of online platforms – a category which, again, does not encompass many types of online games and other digital products.[7] **The DFA should extend these specific prohibitions beyond online platforms by imposing them to all traders providing information society services to online consumers. Furthermore, the DFA should acknowledge the structural effects of personalised commercial practices by considering consumer's vulnerabilities in the light of the influence that the processing of their personal data can have on their decision-making.**

Concerning "addictive designs," the Fitness Check EU consumer law on digital fairness specifically lists "addictive design and gaming" as problematic practices and refers to designs which are often used in games, including: incentives for continued engagement (e.g. badges, rewards) or, conversely, penalties for disengagement (e.g. progress delays, streak losses, or resource losses) as well as interaction-based recommender systems and notifications that are delivered during or outside of the consumer's interaction with the digital product or service.

We agree with the Commission's views that certain designs can induce excessive use of digital products and services, creating potential adverse effects for individuals, especially vulnerable ones such as children. However, research demonstrates that gaming disorder is often the result of a coping mechanism associated with preexisting psychopathology rather than the source of the development or worsening of psychopathology (Falcione & Weber, 2025). Therefore, **the use of the term "addictive" in this context is likely inappropriate.**

"Addictive" refers to "addiction" whose meaning and scope are still debated among experts (West et al., 2023). Major international bodies like the APA, DSM-5, and ICD-10 offer similar but not identical definitions, generally describing addiction as a complex mental condition with multiple factors involved in its development and maintenance – including cognitive, behavioral, and physiological symptoms – that persist despite significant negative consequences (Ahluwalia & Pandey, 2017).

Consequently, **"addictive" designs can be difficult to define and isolate, as they are often the result of a combination of factors, and their effects tend to be contextual (i.e., dependent on the vulnerability of the end user).** The unfairness of a design also often depends on how transparent are the features potentially causing or stimulating addictive behaviours. Hence, while it is important to protect users, especially vulnerable ones, **it is necessary to ensure an evidence-based and consistent definition of what can be seen as "addictive" design**.

[7] In the meaning of Art. 3(i) of the DSA.

Given the above, **we emphasize that any regulatory intervention should be based on scientific evidence of correlation between specific design features and their impact on individual behaviour.** The adoption of broad and ambiguous terms such as "addictive" can result in over-restrictions, especially if they are associated with prohibitions. **We therefore recommend that the Commission consider alternative terms.**

The distinction between "addictive designs" and "dark patterns" also remains unclear. Can "addictive" designs be considered as "manipulative or deceptive designs" prohibited by Art. 25 of the DSA? Could the use of "addictive" designs for commercial purposes be considered as unfair commercial practices under the UCPD? If personal data are used to tailor personalised design with the intention to increase user engagement but potentially result in inducing or stimulating "addictive" behaviours, would the processing of personal data be considered unfair under Art. 5 of the GDPR? Considering the UN Convention on the Rights of the Child, ratified by all EU Member States, the existing EU legal framework and the recognition that children merit specific protection, should these questions be addressed differently when it comes to children and adults?

Recitals 81 and 83 of the DSA refers to "addictive" designs using terms like "design which may cause addictive behaviour" or "design that may stimulate behavioural addictions" and consider these designs as a source of systemic risks in the meaning Art. 34(1)(b) and (d). Pursuant to Art. 35, providers of VLOPs and VLOSEs shall adopt reasonable, proportionate and effective mitigation measures to tackle the risks posed by such designs. However, **such obligation does not extend to smaller online platforms or to services which do not qualify as "online platforms", despite "addictive" designs being present in a wide range of different services within the digital landscape** – including in gaming – therefore, creating a regulatory gap.

We believe that children can be shielded from the negative effects of digital designs through the implementation of appropriate and proportionate measures – for example, by disabling certain features by default when the service is likely to access by children, and by providing parental tools to tailor control of the child's use of the digital product/service to their evolving capacities. In that regard, **we endorse the approach taken in the Brazilian Bill 2628/2022 (Digital ECA)** which – while prohibiting the exposure of minors to certain practices, i.e., loot boxes, profiling and targeted ads – focuses on offering parental supervision tools, including:

- time usage limits and monitoring,
- control over resources (e.g., rewards for time of use, notifications) that may result in excessive use, monitoring of appropriate and healthy use of the product or service,
- restrictions on purchases and financial transactions,
- control over personalised recommendation systems, including the option to deactivate them,
- restrictions and transparent notices about geolocation sharing,
- promotion of digital media education on the safe use of information technology, products or services.

Concerning misleading marketing by influencers, **particular attention should be paid to the interplay between the existing rules addressing the transparency and appropriateness of commercial communication**, notably the obligations imposed to providers of video-sharing platforms under Art. 28b of the audio-visual media services Directive (AVSMD), to providers of online platforms and VLOPs under Art. 26 and Art. 39 of the DSA, and to traders presenting misleading or aggressive commercial communication to consumers in violation of Arts. 5-9 of the UCPD. In particular, **the DFA should clarify the role and responsibilities of influencers in the promotion of a product or a service**, and determine **potential sanctions for misleading commercial communications or the promotion of harmful products or services.**

Improving enforcement through an increased cooperation between relevant stakeholders

a) **Research Data Access & Transparency Reporting**

Effective enforcement relies not only on the capacities of competent supervisory authorities, but also on the broader involvement of civil society and the research community. As noted in our previous feedback to the Commission's consultation on its draft delegated regulation on data access under the DSA, **researcher access to data is essential to uncover systemic risks in digital environments, including risks to consumers' rights in digital games**.

Personalised techniques are often embedded at the system architecture level, invisible from the user interface and inaccessible to consumers, civil society, or researchers (Leiser & Santos 2023). Scrutiny is currently limited to surface-level disclosures in privacy policies and terms of service, which are often kept intentionally broad and vague. The current available information about personalisation techniques is therefore insufficient for meaningful oversight. **To properly evaluate the lawfulness of both data processing activities and associated commercial practices, further disclosure of information on the backend data processing is necessary**.

Art. 40(4) DSA provides data access to vetted researchers who aim to detect, identify and understand systemic risks – such as negative impacts on privacy and data protection, rights of the child, and consumer protection – and to assess the adequacy, efficiency and impacts of the risk mitigation measures. However, this mechanism is confined to VLOPs and VLOSEs, while systemic risks also arise in other digital services, including digital games.

While direct access to user data and systems' codes may pose confidentiality challenges and overburden companies, in particular small organisations, **providers could still be requested to disclose further information on the algorithms embedded in their services which play an influential role on the users' decision-making**. Similar to the transparency reporting obligations laid down in Arts. 15, 24 and 42 DSA with regard to content moderation, **providers of all relevant information society services could be requested to report on the functioning of the algorithmic systems used to foster engagement with their services as well as the implementation of measures to safeguard users, in particular children, from excessive expenditure or use of the services**.

In parallel, the Commission could consider broadening the scope of Arts. 26 and 27 DSA to include transparency and control mechanisms for advertising and recommendations systems used in services which do not meet the definition of "online platform" under Art. 3(i) DSA but still incorporate these features – e.g. digital games.

b) Effective cooperation among competent authorities

In parallel, **crucial attention should be paid to foster effective cooperation between the multiple authorities tasked with the enforcement of overlapping legal instruments.** In a cross-border digital context, isolated enforcement is ill-suited to address systemic breaches and the power imbalance between the most popular, influential online platforms and individual national authorities which often operate on the basis of fragmented regulatory and enforcement powers. Strong cooperation mechanisms should, therefore, be ensured, particularly between the **Consumer Protection Cooperation (CPC) Network**, the **European Data Protection Board (EDPB)**, and **the European Board for Digital Services (EBDS)**, as well as with the **Commission**, to ensure coherent and effective responses to personalised unfair commercial practices in the digital environment. **Clearer institutional cooperation mechanisms should be included in the DFA to strengthen this integrated approach.**

Finally, **the Commission itself should be empowered to take a more direct enforcement role against the most serious and widespread infringements**. Following the DSA model for very large platforms, the Commission could focus on dominant players whose practices have the greatest impact on EU consumers, while national authorities continue to address smaller-scale cases. Such a dual system would preserve the subsidiarity principle while ensuring uniform protection across the Union, shielding consumers from harmful practices regardless of where they are based or which services they use.