Ref. Ares(2025)7044963 - 31/08/2025

Feedback on the European Commission's Consumer Agenda 2025-2030 and Action Plan on Consumers in the Single Market

Who Are We?

We are a subset of experts from the multistakeholder Working Group on Gaming and Regulation, which 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):

- Samantha Bradshaw, American University
- Sara M. Grimes, McGill University
- Kaila Jarvis, Keywords Studios
- Noémie Krack, Centre for IT and IP law (CiTiP) of KU Leuven
- Rachel Kowert, University of Cambridge
- Ingrida Milkaite, Ghent University
- Mariana Olaizola Rosenblat, NYU Stern Center for Business and Human Rights
- Mike Pappas, Modulate
- Martin Sas, Centre for IT and IP law (CiTiP) of KU Leuven, as the main author of this feedback.

Our Position on the Consumer Agenda 2025-2030

We welcome the Commission's initiative, especially regarding its objectives to **strengthen the enforcement** of consumer protection legislation, **protect vulnerable consumers**, and **ensure digital fairness**. These objectives are highly pertinent to the digital games sector, where clearer safeguards could help address manipulative and exploitative practices.

Digital Fairness in the Gaming Context

The Commission's Fitness Check of EU Consumer Law on Digital Fairness has shown the limitations of the existing legal framework, in particular vis-à-vis the protection of EU consumers from harms caused by dark patterns, addictive designs, and unethical personalisation (e.g., via targeted advertising, unfair personal data analysis, and monetization exploiting consumers' vulnerabilities). **These practices particularly affect players of digital games**, who are increasingly exposed to manipulative and exploitative design strategies (Van Rooij et al., 2021).

With the gaming sector now largely dominated by free-to-play business models, game providers depend heavily on revenues from **in-game purchases** and **advertising** (Alha, 2020; Ekambaranathan, et al., 2021). Their profitability therefore hinges on the ability to acquire, retain, and extract monetary value from large numbers of players (Dreier et al., 2017). This dynamic creates strong incentives for game providers to use **manipulative and exploitative design strategies**, notably "dark patterns" (Zagal et al., 2013; Hodent, 2019) and other unfair practices (King et al., 2019), to prolong playtime (thus increasing exposure to advertising) and intensify pressure to make in-game purchases (Petrovskaya & Zendle, 2021).

To maximise the effectiveness of these practices, game providers may **exploit the vast potential of game telemetry**[1] for processing players' data (Sifa et al., 2018). Such processing enables the creation of detailed player profiles (Kroger et al., 2023) and the tailoring of marketing strategies to individual habits and preferences (Ascarza et al., 2024). While such use of telemetry for **personalised marketing** raises significant **privacy and security concerns** (Newman et al., 2014), it also heightens the risk of **exploiting players' vulnerabilities** exposed through **data-driven profiling** (Sax & Ausloos, 2021). The power imbalance between providers' extensive knowledge of players' behaviour and players' reasonable expectations — namely, the belief they are engaging in a ludic space free from surveillance — renders players particularly vulnerable (Dechant et al., 2023).

Recent enforcement actions — such as those launched by the CPC Network against Star Stable Entertainment AB and by the Dutch ACM against Epic Games — have demonstrated that **certain unfair commercial practices commonly used in digital games** (i.e., direct exhortations to children to buy in-game items, pressure tactics such as time-limited offers, deceptive scarcity indicators, lack of clear and transparent information, and failure to clearly disclose the 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**, notably due to a certain disconnection between the current legal framework and realities of the digital environment, an absence of clear technology-specific prohibition or prescription with regard to what can be deemed fair or unfair in specific digital contexts, and an insufficient or inconsistent enforcement of the existing rules. This situation, therefore, calls for regulatory action.

We believe the EU Consumer Agenda 2025-2030 and the upcoming Digital Fairness Act constitute timely opportunities to address these issues. However, these initiatives should **avoid introducing an additional layer of regulatory complexity** and should **rather focus on updating existing rules, ensuring their synergy between the various regulatory initiatives, while securing their effective enforcement.**

---

[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).

Revising of the benchmarks of "average" and "vulnerable" consumers in the age of personalisation

The notion of "**average consumer**" established by the Court of Justice of the European Union (CJEU) in *Gut Springenheide* as being deemed to be "reasonably-well informed, observant and circumspect" does not match **the reality** of everyday consumers whose cognitive biases are subject to manipulative techniques, such as dark patterns (Purnhagen, 2017). **The widespread personalisation of commercial practices further undermines the notion of an informed average consumer** (Duivenvoorde, 2023) as the information asymmetry and power imbalance resulting from the **processing of consumers' personal data now places every consumer in a position of vulnerability** far from the traditional understanding of an observant and circumspect consumer (Drazewski, 2022).

Because the UCPD assesses unfairness through the lens of a "reasonably well-informed, observant and circumspect" average consumer, it **systematically overlooks the structural asymmetries embedded in the system architecture which can induce decisional vulnerabilities** (Helberger, 2022; Leiser & Santos, 2023). These forms of vulnerability are neither marginal nor group-specific, but structural features of the online environment (Riefa, 2022).

A revised framework should, hence, integrate an **architecture-based understanding of vulnerability** that **coexists with and complements group-based protections** (i.e., the traditional categories of vulnerability based on mental or physical infirmity, age or credulity – following the wording of Art. 5(3) UCPD). Such a framework would also account for the fact that unfair personalisation of commercial practices not merely exploit static individual or group traits but rather systematically erode users' decisional autonomy (Zac et al., 2025).

Adopting a more technology-specific regulation to combat dark patterns

The current consumer protection regime heavily relies on **information requirements** and on the **absence of aggressive pressure** (i.e., coercion, harassment or undue influence) to enable the "average consumer" to make informed and autonomous decisions. There is, however, **no further specification** on **how the necessary information should actually be communicated**, nor on the **level of pressure that an "average consumer" would be expected to reasonably resist in a particular context**. This results from the technology-neutral approach taken by these legal instruments.

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.** This ambiguity can be problematic — for example in the detection of unfair commercial practices that involve obscuring information, rather than clearly hiding or omitting it.. **Without further specification on what is prohibited or prescribed, it can be hard to distinguish between acceptable and unacceptable designs.**

According to Rosca, when confronted with technology-neutral provisions, **some regulatees may find creative ways to bypass consumer rights through the design of their interfaces, while others may inadvertently deny such rights** - either due to a lack of knowledge about compliance or because they are constrained by the "servitisation" and "platformisation" of web development, which leaves them dependent on the default settings of third-party solutions (Rosca, 2024). The author also notes that **the uncertainty generated by technology-neutral provisions could make enforcers more hesitant to take action due to fear of legal challenges.**

Rosca thus advocates for **a shift toward more technology-specific mandates with respect to fair designs**. Thus can be achieved, for example, by **integrating dark patterns** that have been identified as harmful to consumers **in the list of prohibited unfair commercial practices under UCPD's Annex I** (see, for example, the dark patterns identified in the ontology developed by Gray et al., 2024). This list could be **kept updated dynamically** to match the pace of a rapidly changing technological landscape. Rather than relying on the lengthy ordinary legislative procedure to amend consumer protection rules, the EU consumer framework (in particular for the UCPD's Annex I and UCTD's Annex II) could be subjected to **periodic reviews**, as envisaged in the new digital acquis. Alternatively, the Commission could rely on faster and possibly more effective mechanisms, such as **targeted amendment procedures (e.g., delegated acts) to introduce prohibitions** and/or **specification of certain design prescriptions (e.g. through implementing acts).** Following the New Legislative Approach, the latter option could also allow for the **involvement of the industry and other relevant stakeholders through (co-)regulation processes**; for example, by making guidelines, code of conducts, or technical standards legally binding.

In the gaming context, the Key Principles on In-game Virtual Currencies issued by the CPC Network in March 2025 constitute valuable examples of technology-specific prohibitions and prescriptions which could be made legally binding. **Upgrading these principles into legally binding technology-specific prohibitions and prescriptions** would allow for a **clearer substantiation of what is allowed or not** by introducing **measurable indicators of unlawfulness** in particular context. It would also create the conditions for potential **automation of the detection and evaluation of legal infringements** (see below).

Expanding the DSA's consumer protection beyond "online platforms"

Several provisions of **the Digital Service Act (DSA) protect users of online platforms against harms which also affect consumers in other types of digital services, including digital games**. Pursuant to the definition of "**online platform**" laid down in Art. 3(i) DSA, **the protection offered by these provisions only applies when the service's principal feature/functionality allows users to disseminate information to the public**. There is, however, **no correlation between the ability to disseminate information to the public and the consumer harms addressed by many of these provisions.** Indeed, these harms also stem from the design of services which do not qualify as "online platforms" due to the absence or the marginality of public dissemination features. As a result, a wide range of digital services, including digital games, unfortunately fall outside the scope of the consumer protection introduced by the DSA (Sas & van der Hof, 2025).

In particular, players of digital games would benefit from the application of the following provisions (Sas, 2024):

- Article 25's **explicit prohibition of deceptive and manipulative designs,** would help address the **widespread deployment of dark patterns in digital games** (Zagal, 2013; van rooij et al., 2021; Fitton et al., 2021; Radesky et al., 2022; Dahlan & Susanty, 2022). That being said, Article 25 is in itself limited to situations which are not yet covered by the UCPD or the GDPR (Art. 25,§2). Given the broad scope of both these instruments, which apply to all B2C transactions or each time personal data are processed, Article 25 seems irrelevant in B2C contexts and has, therefore, raised debates on its actual substance (Santos et al., 2024).
- **Article 26's transparency requirements about the commercial nature of advertisements, holds special** relevance for free-to-play mobile games which rely heavily on ads for revenue, as well as to "**advergames**", which often blur the line between commercial and non-commercial content, potentially confusing players, particularly children, about the commercial nature of certain information. **This strong reliance on advertisement, combined with the ability to massively collect special categories of personal data** (Kroger et al., 2019; 2019b; 2020a; 2020b; 2023) – and, in particular, data related to health (Sas et al., 2025) – **creates a high risk that such data will be exploited for in-game targeted advertising.** Players would, hence, directly benefit from **the prohibition laid down in Art. 26(3), which could be integrated, more generally, into the UCPD's Annex I** to cover all uses of special categories of personal data for advertising purposes, regardless of the qualification of the service in which they occur.
- Article 27's transparency requirements with respect to recommender systems. Beyond ads, players can also be targeted with **personalised offers taking the form of recommendations**. For example, in-game items can be recommended to the player at specific times or be placed in priority in the interfaces of an in-game store in order to nudge the player towards a purchase (Declerck et al., 2024). Although, recommender systems are generally understood as suggesting third-party or user-generated content, Art. 3(s) does not preclude recommendations of information provided by the service provider itself, such as information relating to a commercial transaction. Indeed, **recommender systems play a central role in the personalisation of marketing strategies.** Imposing the requirements of Art. 27 beyond "online platforms" would allow consumers to gain knowledge on the main parameters used in recommender systems and enable them to exercise control over these parameters – therefore, **ensuring a higher degree of behavioural autonomy in their online activities**. Additionally, the increased transparency resulting from the application of Art. 27 would **facilitate the detection of unfair personalised commercial practices** which would have otherwise remained hidden in the system architecture (Leiser & Santos 2023). Hence, extending Art. 27's transparency requirements beyond "online platforms" would help strengthen the enforcement of consumer and data protection regulation (see below). **A revision of the**

Consumer Rights Directive to integrate these information requirements could be envisaged.

- **Article 28's protections for minors – in particular, Article 28(2)'s explicit prohibition of personalised marketing strategies targeting children – which could be integrated into the UCPD's Annex I.** Children make up a substantial share of the gamers demography in Europe (VideoGamesEurope, 2023). However, **the limited scope of Art. 28(2)'s prohibition, being limited to "online platforms", significantly undermines the general protection of minors across all online environments**. While the GDPR takes precedence over the DSA in relation to the processing of children's personal data (Art. 2(4) DSA) and offers a special protection (recital 38), the specific circumstances in which that Regulation permits or restricts the commercial profiling of children are still being debated (Leijten & van der Hof, 2024).

Providing adequate legal and technical tools for detecting and evaluating legal infringements

Enforcement authorities must be equipped with the right tools to address the widespread use of dark patterns online. **Web measurement methods, such as crawling and scraping, show promise in scaling up enforcement capacity by automatically identifying deceptive interface features and linking them to potential legal infringements** (Rosca, 2024). **However, these methods face notable limitations**: they are vulnerable to adversarial website behaviour, are resource-intensive in multilingual markets, and often struggle with the design variability and volatility of digital services. This challenge is particularly acute in the context of digital games, where complex and unique interface designs make automated detection especially difficult. Furthermore, **automated analysis depends on measurable legal indicators of unlawfulness, which are not clearly established under the current technology-neutral legal framework**. Hence, without clearer legal benchmarks, automated tools cannot reliably distinguish between compliant and non-compliant practices. **To strengthen enforcement, more technology-specific regulation should be considered. Establishing design standards or explicitly prohibiting harmful practices would create measurable indicators for automated detection and evaluation of legal infringements.** As discussed above, **a dynamic update of UCPD's Annex I** to integrate identified dark patterns would be a practical step in this direction.

Effective detection and evaluation of legal infringements — or risk thereof — depend on sufficient data access, whether undertaken through manual or automated means. As noted in previous feedback by the Working Group on Gaming and Regulation 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**. Dark patterns and 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 is insufficient for meaningful oversight.

While we argue above that extending the information requirements for recommender systems under Art. 27 DSA beyond online platforms could support the detection of unfair personalised commercial practices, this represents only an initial step. **To properly evaluate the lawfulness of both data processing activities and associated commercial practices, further access to backend processing data is necessary**. Currently, the DSA confines data access obligations to VLOPs and VLOSEs, yet systemic risks listed in Article 34 DSA – such as negative impacts on privacy and data protection, rights of the child, and consumer protection — also arise in other digital services, including digital games. **Restricting data access obligations to VLOPs and VLOSEs risks neglecting harms stemming from services with smaller user bases but which employ equally problematic design practices. We therefore call for extending mechanisms similar to the data access obligations under Article 40(4) DSA to a broader range of digital services, including digital games**. A particular attention should, however, be paid to find a right balance between such data access obligations and privacy, security, intellectual property and trade secret considerations, as well as the available resources of smaller organisations for whom complying with such obligations would be overly burdensome.

Clarifying the legal framework and coordinating enforcement actions

The enforcement of consumer protection rules in the gaming sector illustrates the broader challenges of regulating **an ecosystem situated at the crossroads of several overlapping EU legal frameworks.** Depending on their associated features, digital games can fall simultaneously under the scope of the UCPD, the DSA, the GDPR, or even the Audiovisual Media Services Directive (AVMSD). This multiplicity of regimes, each enforced by different authorities, creates significant confusion and uncertainty for businesses and consumers alike. **Clarifying the legal framework applicable to digital games should be a priority**— for example, by specifying the circumstances in which certain games allowing the creation of user-generated content can be qualified as “video-sharing platforms” under the AVMSD.

In relation to the applicability of the DSA, certain games may not have clear boundaries in terms of the extent to which players may disseminate information to the public. Hence, their qualification as “online platform” under Art. 3(i) DSA largely depends on the appreciation of national enforcing authorities which can potentially diverge and create regulatory fragmentation across the Union. **New legislative interventions, such as the upcoming Digital Fairness Act, should therefore focus on clarifying and coordinating existing obligations rather than creating yet another regulatory layer, which would only add to the legal complexity and risk of fragmentation.**

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. 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 (DSA Board)**, as well as with the **Commission**, to ensure coherent and effective responses to personalised unfair commercial practices in the digital environment.

Finally, **there might be room for the Commission to play a more active role in monitoring and sanctioning the most serious and widespread infringements of EU consumer law**, following the model already established under the DSA in relation to the enforcement against VLOPs and VLOSEs. While this centralisation of enforcement role in the hands of the Commission would require **the UCPD to be upgraded from a directive to a directly applicable regulation**, it would provide the necessary uniformity of rules across the Union. Such a reform would thus enhance legal certainty for businesses and potentially lead to more effective protection for consumers in the fast-evolving digital environment.

Paving the way to the effective redress of immaterial harms at national level

Finally, the effective redress of immaterial harms caused by unfair commercial practices requires clearer recognition at EU level. While the UCPD was originally framed around protecting consumers' economic interests, harmful practices in the digital environment can also result in non-material harms such as loss of time, privacy intrusions, erosion of autonomy, and even emotional distress (ACM, 2022). Although Recital 9 of the UCPD leaves open the possibility for national judges to compensate beyond economic damage, **the reliance on national tort law has created a fragmented landscape, where consumers' ability to obtain redress for the same harm varies widely across Member States** (Santos et al., 2025).

This fragmentation undermines the effectiveness and uniformity of EU consumer law, as it allows businesses to exploit weaker national regimes. It also risks reducing consumer trust in the digital single market as they may face unequal remedies across the Union. **Non-material harms should, hence, be explicitly recognised as redressable under EU consumer protection rules to ensure more consistent remedies across Member States, reduce legal uncertainty, and strengthen trust in digital markets.**