Breaking the extractive digital business model:

a rights-based Digital Fairness Act

EDRi
European Digital Rights

TABLE OF CONTENTS

January 2026

Lead authors: **Dr. Itxaso Domínguez de Olazábal, Jan Penfrat**
Review: Ella Jakubowska, Chiara Casati

Acknowledgements
We are sincerely grateful to our members and partners who have contributed to this document, notably Bits of Freedom, Electronic Frontier Foundation (EFF), Privacy International, SUPERRR Lab, Vrijschrift.org, and Jürgen Bering and Simone Ruf, who supported with the research, conceptualisation, drafting and review of this position paper.

We are also grateful for the generous insights and critical feedback shared by Dr. Gianclaudio Malgieri, Dr. Lorena Sáncez-Chamorro, Dr. Constanta Rosca and the whole ReSocial project, Dr. Monika Namylowska, Dr. Natali Helberger, Dr. Cristiana Santos, Dr. Lex Zard, and Dr. Mark Leiser, whose thinking and contributions have improved the depth and rigour of this research paper.

This paper reflects the position of the EDRi network. EDRi members may publish their own analyses and recommendations with complementary emphases

Acronyms

- Behavioural Design Impact Assessments (BDIAs)
- Consumer Protection Cooperation (CPC)
- Consumer Rights Directive (CRD)
- California Consumer Privacy Act (CCPA)
- Consent Management Platforms (CMPs)
- Digital Markets Act (DMA)
- Digital Services Act (DSA)
- European Commission's (EC)
- General Data Protection Regulation (GDPR)
- Global Privacy Control (GPC)
- Large Action Models (LAMs)
- Representative Actions Directive (RAD)
- Unfair Commercial Practices Directive (UCPD)
- Unfair Commercial Terms Directive (UCTD)
- Very Large Online Platforms (VLOPs)
- Very Large Online Search Engines (VLOSEs)

1. EXECUTIVE SUMMARY AND RECOMMENDATIONS[1]

Digital services influence how people act, make choices and relate to each other and the world. **Many rely on design systems built to control and manipulate behaviour in line with commercial objectives to the detriment of fairness.** Deceptive design, addictive architecture and unfair personalisation shape decisions before people make a choice. These are structural problems. They diminish autonomy and fundamental rights to access information, equality, and data protection, amongst others. **The Digital Fairness Act (DFA) framework should address these issues.**

The DFA should introduce **a new Regulation on structural fairness supported by targeted amendments** to the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD) and the Unfair Commercial Terms Directive (UCTD), alongside strengthened cross-regulatory enforcement."

Current rules were drafted before behavioural targeting, pervasive profiling and self-learning optimisation became standard online practices. While the General Data Protection Regulation (GDPR), the Digital Service Act (DSA) and the Digital Market Act (DMA) address parts of the problem, they do not impose a general duty to design services that respect fairness and autonomy across the market. This gap allows harmful systems to proliferate and providers to profit from manipulation, with direct consequences on fundamental rights. Systems designed around profiling and optimisation undermine meaningful consent, normalise pervasive data extraction and erode the practical exercise of the right to data protection. They also shape what people see, how they engage, and which options remain visible, thereby narrowing autonomy and affecting participation in social and democratic life. **The DFA should address this issue by introducing a structural fairness duty, a hybrid legislative structure and strong cross-regulatory enforcement.**

[1] This position paper draws on EDRi's "A Rights-Based Digital Fairness Act", a longer background paper developed for the Commission's call for evidence on the DFA. This contribution sets out the empirical evidence and legal analysis underlying our proposals, including documented patterns of deceptive design, profiling-based harm and enforcement failures across Member States. It offers the detailed foundation for the structural fairness framework presented in this position paper. "A Rights-Based Digital Fairness Act" is available here: https://edri.org/our-work/a-fair-digital-future-at-risk-edri-contribution-to-the-digital-fairness-act/

1. Structural fairness as the core principle

- Introduce a structural fairness duty that would prohibit all digital services being designed in ways that unfairly exploit or manipulate its users, applicable across the entire DFA framework, governing **interface design**, **personalisation**, **consent flows** and **optimisation systems**.

- Shift the **burden of proof** to traders, requiring them to proof**fairness by design and by default.** This should be combined by **clear prohibitions** with a narrowly scoped **grey list** for context-dependent harms.

- Update the definitions of **"consumer"**, **"trader"** and **"vulnerability"** to reflect digital realities.

- Modernise the definition of **professional diligence** to include a duty to avoid systems that exploit vulnerability.

- Require **behavioural design impact assessments**, **design logs** and **experiment documentation.**

- Adopt the DFA as a Regulation supported by targeted amendments to the UCPD, the CRD and the UCTD, so **fairness obligations** are harmonised and directly enforceable across Member States.

- Anchor structural fairness as a baseline duty precisely because **individual consent, disclosure and vigilance cannot counter system-level manipulation**, shifting responsibility from people to traders by default.

2. Addictive design and attention capture

- Treat **addictive design** as **structurally manipulative** and **presumptively unfair** when theyremoves disengagement cues or uses emotional profiling. **Features incentivising time and/or money should be turned off by default in the baseline mode of use** , and only activated following explicit user choice, with a **single, clearly visible option to deactivate them.**

- Include in the UCPD Annex I a **block list** for tactics that always undermine autonomy and a **grey list** requiring strong justification for high-risk features.

- Ensure that **professional diligence** covers **foreseeable impacts on attention and wellbeing**, with regulators able to assess exposure and optimisation data.

- Make sure that services provide **transparency dashboards** showing time spent, **engagement nudges,** and how nudges are personalised.

3. Deceptive design

- Explicitly apply digital design and behavioural influence in the UCPD **general clause** , covering harms beyond immediate economic loss.

- Prohibit in the UCPD Annex I practices such as **misleading consent interfaces, hidden opt-outs, fake scarcity** and **emotionally manipulative framing** designed to pressure or distort decision-making.

- Ensure that, services **maintain design logs, run fairness tests and complete impact assessments** to demonstrate and evidence compliance for systems that influence decisions, as part of complying with the structural fairness duty.

- Extend a**Accountability should extend across the design chain. Consent Management Platforms (CMPs) CMP providers should be accountable** for manipulative templates, and services should honour machine-readable consent signals.

- Require **equal prominence and equal friction in consumer law** for choices that protect people's rights. Interfaces that make refusal, withdrawal or exit harder than acceptance should be treated as deceptive by design, including through cumulative or cross-step friction.

4. Unfair personalisation and profiling

- **Prohibit the personalisation that exploits protected characteristics**, inferred traits, distress, addiction or economic vulnerability, as part of consumer law

- Guarantee a **non-personalised default** across digital services with full functionality and a right for users to access it in a non-personalised version.

- Make **personalisation opt-in, with unbundled consent.** ensuring that the non-personalised version remains fully functional and free from service degradation.

- **prohibit advertising models based on unlawful tracking or profiling as part of consumer law.** Lawful contextual advertising that does not rely on personal data or profiling must be preserved and clearly distinguished

- **Ensure, through enforcement, that consumer law fully respects GDPR and ePrivacy limits** on covert enrichment and cross-context tracking.

- Bind services to **disclose optimisation objectives, signals and criteria for ranking and recommendations.**

- **Align all personalisation rules with the GDPR and ePrivacy and prevent the creation of new legal bases for processing.** Apply the higher fundamental rights protection whenever laws interact.

5. Breaking the silos: Coordinated, cross-regulatory enforcement

- Introduce a **legal duty of cooperation** between consumers, data protection, competition, media and digital regulators.

- **Support coordinated investigations, evidence sharing and direct Commission enforcement for cross-border manipulation through the Consumer Protection Cooperation (CPC) framework.** Regulators should run joint cases and use pattern-based detection to identify structural manipulation.

- Make accessible to authorities **goal optimisation A/B tests, design logs and behavioural analytics.**

- Introduce in consumer law **presumptions of illegality for repeated practices and presumptions of causality for redress.**

- Ensure that courts are able to apply the law of the forum to **guarantee effective cross-border redress.**

2. WHAT THE DFA IS AND WHY IT MATTERS FOR DIGITAL RIGHTS

Digital services like social media platforms, online marketplaces, streaming services and mobile games, shape how people act, choose and relate by controlling visibility, ranking options and influencing decisions through defaults and recommender systems. They rely on design strategies that influence behaviour in ways people are unaware of, do not expect or do not control. This matters for digital rights because **online design determines whether people can act with autonomy, access information freely and exercise their right to data protection and privacy in practice.**

Features like deceptive design, addictive architecture and unfair personalisation limit these rights by shaping decisions before people can begin to make a choice. The DFA should respond to this structural problem by regulating the design systems that affect rights at scale.

The three interrelated categories of manipulative practices that distort autonomy and fairness online are:

- **Addictive architecture:** it includes feedback loops and interface features that impair people's ability to disengage or exercise time-bound control over their use of digital services.

- **Deceptive design:** this reflects all types of design choices that obstruct or distort consent and decision-making, turning rights into empty formalities.

- **Unfair personalisation:** it includes profiling-based systems that distort decisions or produce discriminatory or exclusionary outcomes (including personalised pricing and discount schemes), restricting equal access to information, services and opportunities.

TABLE 1. Categories of manipulative design and fundamental rights affected

Category	How the practice operates	Fundamental rights affected
Addictive design	Uses feedback loops, recommender systems, defaults and emotional cues to impair disengagement and self-regulation	Human dignity, mental integrity, autonomy, data protection, privacy, freedom of expression and information, democratic participation
Deceptive design	Distorts decisions through misleading interfaces, asymmetric friction, emotional manipulation and consent fatigue	Autonomy, freedom of expression and information, privacy, data protection, access to information, equality
Unfair personalisation	Uses profiling and inferred traits to adapt content, prices, visibility or consent flows	Equality and non-discrimination, data protection, privacy, freedom of expression and information, autonomy, social and economic participation

These practices are not neutral: they are embedded in business models that prioritise data extraction, maximise attention and influence behaviours over people's agency. They interfere with people's freedom to make uncoerced choices, their right to non-discrimination and their ability to participate in democratic and social life without structural manipulation of their digital lives. The DFA must treat them as manipulative by design and regulate them accordingly.

The DFA is a modernisation of the EU consumer law for the digital age. The Digital Fitness Check showed that **current consumer rules were drafted before behavioural targeting, engagement-driven recommender systems and large scale profiling became standard practice.** While the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD), as well as other existing laws, offer important protections, they were not built to address design systems that personalise, rank, and influence behaviour in real time. These regulatory gaps create unequal and opaque environments where people are pressured, confused, or profiled in ways that damage their rights.

Legislators should establish a **cross-cutting duty of structural fairness for all digital services.** It should tackle how services are designed, how choice architectures operate, and how platforms influence people's decisions. This approach aligns with EU fundamental rights. The Charter protects autonomy, human dignity, and fundamental rights to non-discrimination, data protection, privacy, access to information and free expression. Yet, many common design tactics weaken these rights in practice. Manipulative interfaces distort decision-making, profiling extracts sensitive inferences, addictive design pressures attention and affects well-being. **These are rights issues as much as consumer issues.**

Despite claims that the GDPR, DSA and DMA already cover problematic practices, existing laws address only some parts of this problem, In practice, **these instruments have limited and specific scopes, and do not impose a horizontal duty to design for fairness across the market.**

The **GDPR safeguards the right to data protection** and imposes strict limits on profiling and personal data processing[2]. However, it does not regulate how digital environments are designed to steer behaviour, structure choices or exert pressure before any data processing decision is made, nor does it address manipulative design practices that operate independently of personal data.

[2] The DFA must respect these limits. It must not weaken or replace data protection or privacy safeguards. It must not create a legal basis for processing and it must not be used to justify profiling that the GDPR or ePrivacy Directive would not permit. When the DFA interacts with these rules, it should explicitly reaffirm that the higher level of protection for fundamental rights prevails, to ensure legal certainty and avoid regulatory circumvention. This prevents traders from using consumer law to bypass duties under data protection law.

As a result, **harmful design systems remain lawful under data protection rules while still undermining autonomy, equality and the practical exercise of rights.** The DFA could fill a complementary gap by addressing the structural design conditions that normalise data extraction, weaken meaningful consent and cause harm at scale, even in systems that are in formally compliant.

The **DSA** introduces important platform obligations, including a prohibition of certain dark patterns under Article 25, but this intervention is limited to online platforms and framed around specific interface practices rather than a general duty governing the design of everyday choice architectures across all digital services. The DSA **focuses on systemic risks, transparency and content governance rather than on the design of everyday choice architectures** across all digital services.

The **DMA** limits gatekeepers, yet it applies **only to a narrow set of designated firms** and does not address manipulative design as a general market practice. The **Artificial Intelligence (AI) Act** places limits on certain harmful uses of AI and establishes obligations for high-risk systems, but it does **not regulate behavioural influence**, interface design or personalisation outside its risk classifications.

These laws each address specific problems. However, **none of them impose a general duty to design services that respect autonomy and fairness across the entire market.** As a result, structural harms fall between regimes and affect people's rights. Traders exploit these gaps to justify practices that would not pass a unified fairness standard.

TABLE 2. Why existing digital laws do not address structural manipulation

Instrument	Primary regulatory focus	What it structurally does not regulate	Resulting gap
GDPR	Lawfulness of personal data processing and profiling safeguards	Design of digital environments, behavioural steering, collective and pre-contractual manipulation	Manipulative design remains lawful when processing has a legal basis or falls below Article 22 thresholds
DSA	Systemic platform risks, transparency and due diligence	Everyday interface design and behavioural nudging across all digital services	Manipulation persists outside platform risk mitigation
DMA	Market power of designated gatekeepers	Design-driven manipulation by non-gatekeepers and sector-wide business models	Most traders remain free to exploit manipulative design
AI Act	Specific AI uses and high-risk systems	Behavioural influence through optimisation and interface design	Personalisation-based manipulation escapes regulation

The DFA matters because it should fill this structural gap without lowering protections in other laws. Building on the logic of the GDPR, it should reinforce the idea that people should not be pressured into giving up control of their data. It supports the Charter by addressing manipulative practices that undermine real agency. Furthermore, it should strengthen the DSA and DMA by tackling design choices that influence engagement, attention and ranking. It does this by placing responsibility on traders to demonstrate that their design choices respect rights and avoid harm.

A fairness-based approach will also promote equality. Manipulative design[3] often targets or amplifies situations of vulnerability. People facing economic pressure, cognitive load, or marginalisation are more exposed to coercive or misleading interfaces. Profiling practices use sensitive or inferred attributes in ways that lead to discrimination. The DFA has the opportunity to confront these structural inequalities and align consumer law with the EU's broader commitment to equality and non-discrimination.

A robust DFA would also support trustworthy digital markets. Ethical actors are placed at a disadvantage when competitors rely on manipulative patterns. A clear fairness standard restores competition based on value and respect for rights, not on how successfully a service can pressure people.

The DFA matters because it could treat design as a site of power and rights. It acknowledges that digital environments are designed to influence behaviour and that this influence has consequences for autonomy, equality, and data protection. **It can update consumer law to match these realities and strengthen the wider rights framework** without reopening or weakening existing rules.

This brings us to one of today's most pressing policy discussions: the protection of children online. While of crucial importance, this debate is too often framed narrowly, leading policymakers towards flawed solutions, rather than addressing the harmful design of digital environments as a whole. While the protection of children and young people online is essential, **new legislation must be grounded in a commitment to uphold the rights of all people.**

A narrow focus on minors alone risks encouraging inadequate measures, as the ineffective and intrusive age verification, which exclude rather than protect the youngsters, while leaving the broader ecosystem harmful by design. Crucially, it is not only when they go online that minors are harmed. They are also harmed by the online environment, whether or not they are connected: when toxic content and manipulative platforms influence their peers, families, schools, and cultures; when advertising and profiling systems indirectly target them through others; when default designs normalise surveillance, addiction and commercial exploitation as acceptable standards. **Ensuring that digital services are fair and safe by design for everyone would create an internet that protects minors and their rights meaningfully**, without isolating them or pushing them into riskier, more opaque spaces.

[3] Manipulative design refers to interface or system level choices that steer behaviour by exploiting cognitive shortcuts, situational pressure or information asymmetry. It covers design that has the likely effect of influencing decisions against a person's interests or intentions. The term highlights that manipulation is produced through design logic, not through isolated features. Manipulative design is therefore a structural problem and a rights issue, as it directly affects autonomy, equality and the exercise of data protection rights.

3. STRUCTURAL FAIRNESS AS THE CORE PRINCIPLE

Structural fairness should be the organising idea behind the DFA. Digital services steer and constrain people's behaviour through interface design, default settings, ranking systems and personalisation. These systems influence people in ways they cannot detect or resist. **Fairness cannot rely on individual vigilance. It must be built into the system from the start.**

Structural fairness should be a legal duty for traders and all other actors who design, deploy or determine digital services. Such principle would bind them » to ensure that interface design, defaults, optimisation and personalisation systems do not exploit vulnerability or undermine autonomy and fundamental rights. **Traders must design and operate services in ways that respect fundamental rights.** Digital environments often work through behavioural pressure. People face nudges, timers, friction and hidden pathways thatinfluence them without their awareness. Disclosure or consent flow can not counter this alone. A structural duty is needed because the harms are structural.

This principle aligns consumer law with the Charter. Human dignity, autonomy, non-discrimination, freedom of expression and data protection, among others, require environments in which people can meaningfully control their experiences. Manipulative design weakens this control. Profiling extracts sensitive inferences. Personalisation creates unequal pathways. Addictive interfaces pressure attention. These practices erode the real exercise of rights.

TABLE 3. From individual choice to structural fairness

Current model	Structural fairness model under the DFA
Individual vigilance	Fairness by design and by default
Disclosure and consent	Design accountability and system-level assessment
Case-by-case illegality	Pattern-based presumptions
Burden on people	Burden on traders

EDRi's key recommendations

1. A hybrid legislative architecture

Structural fairness needs a hybrid legal structure. **The DFA should be a regulation with self-standing provisions,** accompanied by targeted amendments to the UCPD, the UCTD and the CRD, and complemented with an ambitious revision of of the CPC regulation. This would allow the regulation to introduce new rights-based obligations, such as fairness by design and non-profiling by default, while aligning existing directives with the realities of digital markets. This approach would also ensure a coherent enforcement system in which the Commission plays a direct role, as in the DSA, and avoids uneven transposition across Member States.

2. Modernising legal concepts: why definitions matter.

Structural fairness requires concepts that reflect digital realities.
Consumers should include all people whose interactions with a digital service are monetised or otherwise exploited for commercial value, including through profiling or personalised interfaces, whether or not they pay for a service. The UCPD relies on the notion of the "average consumer" to assess unfairness. In digital environments, this benchmark no longer reflects reality.
Behavioural design exploits fatigue, time pressure and information asymmetry that affect most people. In light of this, **the concept of vulnerability should be introduced to reflect widespread, situational vulnerability users are exposed to**. This principle should be understood as systemically induced, rather than just a fixed individual characteristic. It emerges from interactions between users' characteristics, situational conditions and exploitative design environments. It includes structural and situational factors.

In this sense, it is critical to take into account that **recognising situational vulnerability does not replace existing categories of vulnerability,** such as age, disability or economic dependence, but rather expand them to reflect how digital design can create or intensify vulnerability across a much broader range of people and contexts. Thus, exposure to manipulation is not evenly distributed, it is intensified – structurally and contextually – for certain groups and communities.

This is why **the UCPD's concept of "average consumer" should be updated** to reflect widespread, situational vulnerability and justify higher protection given how many digital services rely on behavioural influence and structural power imbalances.

Regulators should focus on how digital systems create and intensify vulnerability rather than treating it as fixed or exceptional. It is critical to understand that vulnerability is not a narrow category. It is shaped by context, power and design. Digital systems can create or amplify vulnerability by exploiting situations in which people are tired, distracted, or overwhelmed by time pressure, financial stress, or repeated prompts demanding immediate decisions. A modernised legal vocabulary prevents practices that exploit or intensify these conditions.

The DFA should define "traders"to include all entities that provide, deploy or determine the operation of digital services. This definition should extend to developers of recommender systems, providers of AI infrastructure and intermediaries whose design or optimisation choices shape interaction or decision-making, regardless of any direct contractual link with the end user.

The UCPD should be modernised to ensure that professional diligence reflects digital systems, including optimisation models, profiling, and interface design that influence behaviour. Traders should meet a standard that incorporates fairness by design, respect for data protection and predictable treatment across interfaces. A modernised definition must reflect the reality that traders operate optimisation systems that influence behaviour.

Professional diligence must therefore **include a duty to design services that do not mislead or pressure people**, and **a duty to avoid systems that exploit structural or situational vulnerability**. Professional diligence should explicitly include fairness by design and by default[4]. Behavioural influence, consent flows and personalisation systems form part of the trader's professional conduct. A trader that deploys interfaces or optimisation systems that exploit vulnerability or undermine informed decision-making should be presumed to have breached professional diligence under the UCPD.

[4] We're grateful to the European Consumer Organisation (BEUC) for being the first civil society organisation to introduce this terminology, and for their long-standing, outstanding work on digital fairness in consumer law. See, for example, their position paper "Towards the Digital Fairness Act" https://www.beuc.eu/position-paper/towards-digital-fairness-act

3. A structural fairness duty

Under the new framework, the responsibility for structural fairness must shift. **People who must navigate systems designed to influence them must not bear the burden. Traders must prove that their design choices are fair, necessary and proportionate and, most importantly, rights-respecting.** Regulators today must show that a pattern is unfair. Traders exploit this and present their practices as neutral. A burden-shifting model would reverse this imbalance. Instead, traders would be requested to prove that their design supports, rather than undermines, autonomy and rights. Additionally, when a trader has been found to use an unfair or manipulative practice, the future use of the same or a materially similar practice in the future should be presumed as unlawful.

A fairness duty would clarify that fairness is not a procedural formality, but rather a structural obligation rooted in fundamental rights. This duty must apply to interface architecture, consent and personalisation flows and profiling based interaction models. It must require traders to justify systems designed to predict, steer and constrain people's behaviours, rather than forcing people to resist them.

Consumer law should introduce presumptions of illegality and causality when a trader repeats a previously sanctioned practice or when structural manipulation produces foreseeable harm. When an authority has deemed a practice as illegal, then the same practice used by the same trader should be presumed illegal in new investigations. People should also benefit from a presumption of causality in redress actions. These presumptions would strengthen enforcement and stop traders from rebranding the same harmful design under new labels. They would also shift the burden of proof to traders, requiring them to prove that a design system is fair, necessary and lawful.

Instead**, legislators must require fairness by design and by default to turn this principle into practice.** Fairness by design and by default means that digital services must be built and configured in ways that do not rely on behavioural pressure, manipulation or exploitation of vulnerability as a normal mode of operation. Traders should be required to ensure, ex ante, that default settings, interface architectures and optimisation strategies respect autonomy and do not produce structural disadvantage or interfere with rights.

Compliance should not depend on disclosures or user vigilance. When systems influence decisions, traders must be able to demonstrate that design choices, defaults and optimisation practices are necessary, proportionate and compatible with fundamental rights. Practices that are unfair by design should be prohibited outright, rather than subject to conditional justification[5].

[5] This approach mirrors the established EU regulatory logic in data protection law, where obligations such as data protection by design and by default require controllers to prevent foreseeable harms through system configuration and default settings, rather than relying on individual consent or downstream mitigation. Applying a similar preventive logic to consumer protection ensures that fairness is embedded at the level of design and operation, not left to individual resilience.

4. UCPD tools: General clause, block lists and targeted use of grey lists

The UCPD already contains a general clause that bans practices that mislead, pressure or manipulate people. The DFA should **confirm that this clause applies to digital interface design, behavioural influence and data-driven personalisation, and that it captures harms beyond immediate economic effects.** Clarifying this scope would update the clause for digital markets and ensure it covers evolving forms of manipulation.

Annex I should be expanded to include **block lists banning design practices that are unfair by design** and are incompatible with autonomy. Examples include misleading consent interfaces, emotionally coercive framing or cancellation tunnels. These practices should be **prohibited outright**, as their primary function is to mislead or pressure people.

Grey lists should be used only where harm is not intrinsic to the design practice itself but arises from cumulative optimisation, intensity or deployment at scale. This is often the case with engagement-driven or addictive design, for example where notification frequency, recommender pacing or reward mechanics are continuously adjusted to maximise time spent. In such cases, grey listing should operate through a **presumption of unfairness, shifting the burden to traders** to demonstrate that the design does not impair autonomy, exploit vulnerability, or undermine the ability to disengage. Grey lists are not appropriate for deceptive design practices whose function is manipulation rather than engagement.

Together, the general clause, block lists ,and targeted use of grey lists would allow the UCPD to operationalise structural fairness while distinguishing between practices that are inherently unfair and those whose harmfulness depends on how they are deployed.

TABLE 4. Block list and grey list as enforcement tools

Legal tool	Type of practice	Legal effect	Trader obligation
Block list	Structurally manipulative practices	Automatically prohibited	Must not deploy
Grey list	High-risk design practices	Presumed unfair unless justified	Demonstrate necessity and proportionality
General clause	All other commercial practices	Unlawful when unfair	Meet digital professional diligence

5. Operational safeguards and behavioural design impact assessments

Fairness also requires operational safeguards. In the new framework, traders should conduct feature-level risk assessments, maintain design and experiment logs. They should also provide regulators with audited evidence showing how interfaces, prompts and personalisation systems affect autonomy and equality.

Where profiling, personalisation or opaque optimisation are used, there should be a presumption of unfairness[6]. **Traders should complete Behavioural Design Impact Assessments (BDIA) and show that systems are necessary, fair and safe.** Regulators should have access to documentation on system objectives, design decisions and foreseeable effects. These measures would make fairness enforceable and stop traders from deploying design choices that cannot be explained or justified.

Structural fairness is forward-looking and does not depend on a specific technology. It applies to any design, interface or personalisation system that shapes behaviour. It is a concept that protects people across emerging environments without lowering existing rights.

This concept would recognise digital environments as systems of influence. It would set the standard for services built to respect rights. It would anchor the DFA by centring fundamental rights, modernising consumer law, shifting responsibility onto traders and creating tools to limit harmful design.

TABLE 5. Enforcement logic and burden of proof under the DFA

Today	Under the DFA
Authorities must prove unfairness	Traders must justify design choices
Limited access to evidence	Mandatory access to design logs and optimisation data
Reactive enforcement	Preventive and corrective enforcement

[6] Our Background Paper elaborates on all the criteria BDIAs should meet, in line with the work done on other types of Impact Assessments.Here the "Framework for meaningful engagement; human rights impact assessment of AI" published by the European Center for Non-for-Profit Law: https://ecnl.org/publications/framework-meaningful-engagement-human-rights-impact-assessments-ai

4. ADDICTIVE DESIGN AND ATTENTION CAPTURE

Addictive design shapes how people spend time, attention and energy online[7]. Many services rely on mechanisms built to maximise time spent, not to support autonomy or well-being. These mechanisms create loops of compulsive engagement. They trigger behavioural responses through timers, streaks, infinite scrolling, personalised prompts or variable rewards[8], which make it harder to stop, encourage repeated checking, or nudge people to stay longer than they intended. **People experience this without seeing how these systems work.** This pressure undermines autonomy and interferes with the exercise of rights.

Addictive design should thus be recognised as structurally manipulative and presumptively unfair when it removes disengagement cues, uses emotional profiling to trigger compulsive feedback loops[9] or interferes with boundaries set by individuals.

Attention capture is not a side effect, it is a commercial strategy. Increasingly so, services are optimised for metrics like retention, session length, and click probability[10]. Interfaces adjust to individual behavioural patterns. Predictive systems identify when people are most likely to continue scrolling or keep watching. These systems create a structural imbalance. Traders hold the data, the predictions, and the design power. People are faced with a system built to extract as much their attention as possible, even if it harms their well-being.

These practices raise fundamental rights concerns. **Autonomy and dignity** suffer when people cannot meaningfully disengage. The right to data protection suffers because engagement systems often rely on profiling. Personalisation engines monitor behaviour to guess when people are tired, stressed or more easily influenced, and adjust prompts or content to keep their attention. This **undermines free and informed decisions** about data use and many other aspects, and produces environments where consent is weakened or bypassed through constant design pressure. Engagement-driven recommender systems also affect **freedom of expression** by deciding which voices are amplified, which content is sidelines, and how widely ideas circulate. People do not see the same information. They see what keeps them engaged. This creates structural distortions in **access to information.**

[7] This paper builds on and aligns with the European Parliament's 2023 resolution on addictive design and consumer protection (P9_TA(2023)0459) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html , which recognises the growing evidence of systemic manipulation in digital interfaces and the need for a comprehensive regulatory response

[8] Timers are countdowns that create urgency. Streaks reward repeated use and signal loss if a person stops using the application. Infinite scrolling removes natural stopping points by continuously loading content. Personalised prompts are notifications or messages tailored to predicted behaviour. Variable rewards deliver outcomes unpredictably, encouraging repeated engagement. These features are widely used to prolong attention and increase return.

[9] Compulsive feedback loops are design mechanisms that repeatedly reward or prompt behaviour in ways that encourage continued use, making it harder for people to disengage even when they intend to stop.

[10] Retention refers to how often people return to a service. Session length measures how long people stay each time they use it. Click probability estimates how likely a person is to click on a piece of content or option. These metrics are commonly used to optimise design choices towards prolonged engagement.

These harms are often context-dependent, with certain groups, such as children and teenagers and neurodivergent people, **more exposed to behavioural pressure**, even if all people are structurally vulnerable to engagement maximising. Engagement systems often identify patterns linked to developmental stages, sleep cycles, or states of emotional vulnerability. This repeatedly exposes young people to behavioural pressure. It also affects equality. People under economic stress, experiencing isolation, or facing structural disadvantages are more likely to be drawn into engagement loops that are hard to break. **Addictive design amplifies existing situations of vulnerability.**

TABLE 6. Forms of addictive design cross digital services

Area affected	How addictive design operates in practice	Rights interference
Attention and time spent	Continuous content delivery through infinite scroll, autoplay or feed replenishment that removes natural stopping points	Autonomy, mental integrity, dignity
Frequency of return	Push notifications, reminders or prompts designed to trigger habitual checking or fear of missing out	Autonomy, freedom of thought, mental integrity
Intensity of interaction	Streaks, reward ladders, badges, likes or progression systems that penalise breaks and encourage prolonged engagement	Autonomy, well-being, dignity
Decision-making and self-regulation	Design patterns that override or weaken user-set limits, pauses or controls	Autonomy, data protection, dignity
Decision timing and availability	Disappearing or time-limited content designed to create fear of missing out	Autonomy, freedom of thought, access to information
Behavioural optimisation at scale	A/B testing, experimentation and dynamic adjustment of interfaces to maximise engagement metrics over time	Autonomy, freedom of thought, human agency
Emotional and situational vulnerability	Re-engagement prompts or interface changes triggered by inferred boredom, distress, fatigue or hesitation	Autonomy, mental integrity, equality
Economic exposure within engagement systems	Loot boxes, in-game currencies or monetised reward loops embedded in engagement-driven environments	Autonomy, consumer protection, economic participation

EDRi's key recommendations

The DFA should **address these harms by regulating attention capture as a structural issue**. The goal is not to police individual features, but to control design systems that steer people's behaviour at scale. EDRi proposes clear obligations:

1. Require opt-in for engagement-driven features

Engagement features should be opt in. For the purposes of the DFA, engagement features are design elements whose primary function is to increase time spent, frequency of return or intensity of interaction, rather than to enable the core functionality of the service. People should not be forced into recommender systems or interfaces built to maximise time spent.

An opt-in model reduces behavioural pressure and restores a measure of self determination. It also aligns with EU data protection law, which limits profiling without freely-given consent. In this regard, engagement-driven features, including autoplay, infinite scroll, personalised prompts and streak systems, should be switched off by default. Any activation must require clear, unbundled opt-in.

Alongside this, where engagement-driven features are offered, **services should provide an easy, clearly visible and persistent option to deactivate them at any time**, without penalty or loss of functionality. In this regard, given that recommender systems or algorithmic curation are used to maximise engagement, people should also be able to opt out and access alternative content delivery options that do not rely on engagement optimisation.

2. Adapt the UCPD general clause and introduce an updated block list for high-risk tactics

The DFA should **broaden the UCPD general clause to cover any design practice that has the likely effect of pressuring attention.**

Alongside this general clause, an amended **block list should be included in the UCPD Annex I for design tactics that always interfere with autonomy.** These tactics include variable reward loops, forced autoplay, default activation of push notifications, streaks that penalise breaks, and timer-based prompts that pressure immediate return. These tactics have no legitimate justification, as they undermine agency in ways that cannot be mitigated through transparency alone.

3. Treat some forms of context-dependent risks as structurally unfair

The UCPD should also **include a grey list of high-risk engagement practices, requiring traders to justify any behavioural influence features that could create foreseeable pressure.** These are practices that involve strong behavioural influence. Examples includes personalised prompts designed to trigger fear of missing out, event-driven notifications that encourage compulsive checking, reward ladders, or dynamic difficulty spikes that prolong play or scrolling[11]. Traders using these features should face a strong burden of proof: they must show the feature is necessary, proportionate, and compatible with rights. This reverses the current model in which traders deploy behavioural techniques without demonstrating safety.

Grey listing is only appropriate for certain engagement-driven practices where harm is not inherent to the feature itself but arises from cumulative optimisation, intensity and deployment at scale. This logic does not apply to deceptive design practices, which primarily function to mislead or pressure people, and which should therefore be prohibited outright.

TABLE 7. Addictive design practices: prohibited and presumed unfair

Practice	Structural feature	Legal treatment	Justification
Infinite scroll and forced autoplay without controls	Removes stopping cues and prevents disengagement	Block list	No legitimate function beyond maximising time spent
Compulsive feedback loops and streaks	Exploit reward anticipation and penalise disengagement	Block list	Designed to induce dependency and loss of control
Default activation of push notifications	Forces engagement without prior choice	Block list	Imposes behavioural pressure by default
Timer-based prompts and urgency cues	Pressure immediate return or continued use	Block list	Exploit time pressure and attention bias
Loot boxes with monetisation	Variable-ratio rewards and obscured costs, combined with spending incentives	Block list	Exploit gambling-like dynamics and economic vulnerability
In-game currencies without real-money equivalence	Obscure real costs and spending consequences	Block list	Misleads and exploits vulnerability and behavioural bias
Emotion-triggered re-engagement prompts	Uses inferred boredom or distress, or fear of missing out	Block list	Targets vulnerability by design
Persistent override of user-set limits	Undermines self-regulation	Block list	Circumvents expressed user intent
A/B testing optimising engagement or spending	Behavioural experimentation	Grey list	Legitimate in limited contexts only - harm depends on cumulative optimisation and intensity
Notification frequency optimisation	May support usability or addiction - adjustment of prompts and alerts over time	Grey list	May support core functionality but risks attention pressure at scale
Dynamic difficulty or content pacing spikes	Artificially prolong interaction or play	Grey list	Creates dependency through escalation mechanics

[11] Reward ladders offer escalating rewards that encourage continued engagement by penalising stopping. Dynamic difficulty spikes adjust challenge levels in response to behaviour, increasing pressure at moments likely to keep people engaged.

4.Operationalise diligence to protect attention

The UCPD should clarify that **professional diligence includes assessing foreseeable impacts on attention and well-being of environments optimised to influence behaviour.** This clarifies and modernises an existing duty. A service that systematically pressures attention violates the right to use digital services without harm. A duty of care creates a **baseline expectation**. Traders must assess the foreseeable effects of their design choices, set exposure limits , reduce the intensity of behavioural triggers when risk is identified and provide clear pathways to stop or reduce engagement. Regulators should be able to request assessment reports, monitor exposure data and require design changes when pressure is excessive.

5. Provide transparency on engagement dynamics

The DFA should require **transparency dashboards for time spent and engagement nudges**. People deserve clear information about how much time they spend, what nudges they receive, and how these nudges are personalised. This supports informed choices and allows regulators to understand how influence operates across systems.

Video games: a clear example that manipulative practices go beyond platforms

Video games show clearly that harmful digital design is not limited to platforms. They illustrate how digital services outside traditional social media use optimisation systems, behavioural tracking and reward mechanics to influence decisions at scale. Games do not fit the common narrative that manipulation only happens on very large platforms. They demonstrate that addictive architecture is a structural feature of digital services in general, not a platform-specific issue. Similar engagement and monetisation mechanics are also found in other digital services, including streaming platforms, social media, fitness apps and online marketplaces.

Many games rely on variable reward loops, difficulty spikes and progression systems designed to keep people engaged for extended periods of time. Premium virtual currencies obscure real prices and make spending harder to track. Loot boxes that require payment create uncertainty that resembles gambling and exploit reward anticipation. Pay-to-progress or pay-to-win systems condition advancement, competitiveness or access to content on spending rather than skill or choice. These features influence behaviour and drive repeated play and spending.

Children and teenagers face even stronger risks. Engagement systems identify patterns linked to developmental stages, fatigue or emotional vulnerability, making it easier for games to trigger compulsive loops. Many adults feel pressured when games introduce time-limited offers, competitive disadvantages or pathways designed to create a sense of urgency or fear of missing out. These systems amplify both structural and situational vulnerability.

The DFA should recognise these mechanisms as forms of addictive design. A block list should prohibit loot boxes that require payment and reward loops built on uncertainty. It should also prohibit premium virtual currencies that obscure real-world spending and make loss of control more likely. All in-game purchases must display real currency values, including where virtual currencies are used as intermediaries. A grey list should apply to game mechanics that drive compulsive returns or spending through optimisation and intensity. In-game purchases should be opt-in only and must never be linked to access to essential functionality. These measures align with the DFA's fairness duty by stopping design systems that overwhelm autonomy and exploit vulnerability.

5. DECEPTIVE DESIGN

Deceptive design covers interface choices that mislead, pressure, or confuse people[12]. It has become one of the most visible and pernicious expressions of manipulation in digital markets. The term describes design that manipulates decisions through visual tricks, interface's structure (how options are organised and presented) or timing. These choices interfere with free and informed decision-making. They distort how people exercise their rights and they weaken trust in digital services.

Deceptive design is widespread because it works. It increases conversions (e.g. getting people to buy things), limits cancellations (e.g. of subscriptions), and extracts more data. The DFA must address it as a structural rights problem, not as a marginal issue.

Deceptive design takes many forms. Examples are confusing button layouts, hidden unsubscribe routes, interruptions that steer people away from privacy-protective choices, and mismatched colours that draw attention to the option that benefits the trader. But also other deceptive design are repeated prompts that exhaust people into accepting tracking, and applications that force continuity, where subscriptions renew automatically and cancellation is made difficult or confusing, trapping people in subscriptions. These tactics exploits cognitive shortcuts and overwhelm people's ability to evaluate choices.

These patterns, well exemplified by the 'Consent or Pay' models , also create the so-called 'cookie fatigue.' People face repeated prompts designed to push them towards accepting tracking. Fatigue becomes a design tool. The problem is not consent itself, but rather the interface built to defeat autonomy. Cookie fatigue shows how interface manipulation can replace meaningful choice by use of deception.

These harms are a major and unaddressed gap in European consumer law that has negative effects for fundamental rights. However, this issue can be fixed. **The Charter requires environments in which people can act based on clear and accessible information. Deceptive design does the opposite.** It exploits confusion and fatigue to obtain acceptance that is neither free nor informed.

Deceptive design also reinforces inequality. People with less time, less digital literacy, or who are juggling multiple pressures are more exposed to misleading interfaces that demand attention, comparison and repeated decisions. Groups facing structural discrimination – such as people on low incomes, racialised communities, people with disabilities or older people – are more likely to encounter additional

[12] The term describes design that manipulates decisions through visual tricks, structure or timing. We use this expression instead of 'dark patterns' because it focuses on the practice, its impact on the rights and the duty of fairness. To define the same practices, it is also used the term "dark patterns", which is a popular label, but does not capture the legal and behavioural analysis needed for regulation. Deceptive design is about power, influence and interference with autonomy. See for instance H. Brignull, Deceptive Patterns (Testimonium Ltd, 2023) and Mark Leiser, Dark Patterns, Deceptive Design, and the Law (Hart Publishing, 2025).

friction, more confusing choices, and repeated prompts. This is because these design systems exploit existing inequalities in access, time and resources. The DFA needs to address this inequality as part of its fairness duty.

The current legal framework is inadequate. The UCPD bans "deception", yet this was intended for static, pre-digital markets and it fails to capture dynamic interfaces, personalised nudges, or design that shifts based on behavioural predictions. While the GDPR requires valid consent, it cannot on its own address the full ecosystem of interface design, defaults and behavioural pressure that shape people's decision-making before any consent is given. Similarly, the DSA addresses some manipulative design on large platforms, but its scope is limited and it does not cover the full range of services or tactics found across the market. **These gaps allow deceptive systems to flourish.**

TABLE 8. Common forms of deceptive design across digital services

Category	How deceptive design operates in practice	Rights interference
Consent and agreement	Interfaces that steer acceptance through unequal button size, colour or placement, default opt-ins, or hidden refusal options, or default addition of products or services to the basket without clear and informed consent	Autonomy, data protection, freely given consent
Choice architecture	Asymmetric friction, forced pathways or pre-selected options that make rights-protective choices harder to access	Autonomy, equality, access to information
Withdrawal and exit	Cancellation tunnels, hidden unsubscribe routes, repeated confirmation steps or misleading prompts discouraging exit, or interfaces where buttons or labels lead to outcomes different from what users reasonably expect	Autonomy, consumer protection, freedom of contract
Decision timing and urgency	Countdown timers, fake scarcity claims, urgency cues or time pressure that distort decision-making	Autonomy, freedom of choice, access to truthful information
Emotional manipulation	Confirm-shaming, guilt-based language or fear-inducing prompts designed to exploit emotional responses	Dignity, autonomy, freedom of thought
Information transparency	Fragmented disclosures, obscured terms, ambiguous or confusing wording (e.g. double negatives), misleading price presentation or drip pricing	Access to information, economic participation
Onboarding and defaults	Initial set-up flows that steer people into personalised, data-intensive or paid modes by default	Autonomy, data protection, equality

EDRi's key recommendations

The DFA must modernise this area by introducing clear and enforceable duties.

1. Clarify the UCPD general clause for digital design

The DFA should clarify and operationalise the existing UCPD general clause by explicitly confirming that it applies to digital interface design, behavioural steering and data-driven manipulation. **Any design practice that is likely to mislead or pressure people should be treated as unfair**, including practices that render consent meaningless . This clarification must cover evolving forms of manipulation and prevent traders from evading liability through novel interface techniques or technical complexity.

Accountability should extend across the design chain. Providers of consent management platforms (CMPs), interface templates and standardised frameworks should be held responsible for enabling or deploying manipulative designs at scale. Technical implementation must not be used to undermine the exercise of rights.

2. Require equal prominence and equal friction for choices

Consumer law should require that options protecting people's rights are presented with equal prominence and equal friction. Interfaces that make refusal, withdrawal or exit harder than acceptance should be treated as deceptive by design. This principle should apply to all areas in which consent is given, such as subscription management, account settings and any interface governing access to rights.

To this end, the CRD should explicitly require that subscription cancellation and withdrawal are available through a simple, single and clearly visible action, without additional steps, misleading prompts or unnecessary delays. Designs that rely on cumulative friction to discourage refusal or exit should be presumed to be incompatible with professional diligence.

3. Prohibit deceptive design practices that are unfair by design

Alongside the clarification of the general clause, **the UCPD Annex I should be expanded to include a clear list of deceptive design practices** that are always unfair and should be prohibited outright. These are practices have the primary function to pressure, mislead or exhaust people into accepting outcomes that are contrary to their interests and that cannot be made compatible with autonomy through transparency or consent.

This block list should include:

- misleading consent interfaces with unequal visual weighting;
- default opt-ins for data sharing or personalisation;
- confirm-shaming and emotional pressure;
- forced continuity and obstructed cancellation pathways;
- fake scarcity signals and countdown timers;
- personalised or adaptive consent flows;
- prompt fatigue systems;
- disguised switching costs such as pay-to-cancel designs;
- and deceptive onboarding flows that steer people towards data-intensive modes.

These practices systematically undermine free and informed decision-making and should therefore be treated as always unfair.

TABLE 9. Deceptive design practices under the DFA: practices that should be prohibited

Practice	How manipulation operates	Recommended legal treatment under the DFA
Misleading consent interfaces, including oversized accept buttons and hidden reject options	Visual imbalance and asymmetric friction steer decisions	Prohibited - Renders consent meaningless and undermines autonomy
Confirm-shaming, guilt framing and emotional pressure	Emotional coercion replaces free choice	Prohibited - Interferes with freedom of decision-making and dignity
Forced continuity, hidden unsubscribe routes and obstructed cancellation	Cumulative friction prevents exit	Prohibited - Traps people in unwanted contractual relationships
Countdown timers, fake scarcity and urgency cues	Manufactured pressure distorts judgement	Prohibited - Misleads and exploits cognitive bias
Default opt-ins for data sharing or personalisation	Pre-selection removes meaningful choice	Prohibited - Circumvents data protection and consumer safeguards
Personalised or adaptive consent flows	Behavioural steering based on profiling or inferred willingness	Prohibited - Exploits asymmetry and undermines freely given consent
Prompt fatigue and repeated resurfacing of rejected choices	Decision exhaustion overrides resistance	Prohibited - Targets fatigue and undermines autonomy
Disguised switching costs, pay-to-cancel designs or security theatre	Hidden penalties discourage refusal or exit	Prohibited - Exerts coercive pressure through design
Deceptive onboarding flows steering people toward personalised or data-intensive modes	Early-stage behavioural locking-in	Prohibited - Exploits dependency at moments of vulnerability

4. Ensure effective enforcement through design-level assessment

The DFA should **ensure that enforcement focuses on design logic and functional effects**, rather than on isolated interface elements or formal disclosures. Authorities should be empowered to assess whether a design pattern, taken as a whole, is likely to mislead or pressure people, including through cumulative or cross-interface effects.

Traders should be required to document and retain information on design choices, behavioural testing and optimisation strategies that affect user decisions. Claims of usability, efficiency or commercial necessity should not be accepted if a design operates through pressure, exhaustion or emotional manipulation. This approach prevents enforcement from being reduced to superficial compliance checks and reflects how manipulation operates in practice.

5. Introduce presumptions against repeated and template-based manipulation

The DFA should **introduce clear presumptions against the repeated or template-based use of deceptive design practices.** Where a trader has been found to deploy a prohibited manipulative pattern, the reuse of the same or materially similar design should carry a presumption of unlawfulness, regardless of minor visual, technical or contextual changes. Likewise, the use of standardised templates, consent frameworks or interface components that reproduce prohibited patterns across multiple services should trigger a presumption of illegality. Traders should not be able to relabel, slightly modify or repackage manipulative design in order to evade enforcement. Regulators should be empowered to assess practices at the level of design logic and behavioural effect, reflecting the iterative and scalable nature of manipulation in digital markets.

6. UNFAIR PERSONALISATION AND PROFILING

Personalisation shapes what people see, how they navigate services, and which options they reach. Profiling use predictions about behaviour and infers traits to adjust content, prices, or pathways. These systems create unequal environments where different people receive different experiences based on data that they do not control.

Many of these practices undermine, among others, the fundamental right to data protection and reduce the space for free and informed decisions, and have a considerable negative impact on users' trust. Moreover, while often these practices are presented as enhancing relevance, they can limit autonomy, reinforce market asymmetries, and normalise hidden influence, turning adaptive design into a mechanism of structural manipulation.

TABLE 10. Forms of unfair personalisation across digital services

Area affected	How personalisation operates in practice	Rights interference
Content and ranking	Personalised ordering, filtering or suppression of content based on profiling, inferred interestWs or behavioural predictions, including but not limited to recommender systems	Freedom of expression and information, pluralism, safety
Pricing and discounts	Personalised prices, discounts or fees based on profiling, device or behavioural signals, including dynamic adjustments during the purchasing process	Equality and non-discrimination
Access and visibility	Differential access, visibility or friction based on inferred characteristics, past behaviour or predicted value	Equality, social, political and economic participation
Consent flows	Adaptive consent prompts, timing or presentation based on profiling, behavioural signals or inferred willingness to agree	Data protection, autonomy, freely given consent

Unfair personalisation covers both content and price personalisation. It occurs when services use inferred or sensitive traits, such as health status, sexual orientation, religious belief, political opinion or indicators of financial distress, to steer behaviour. It includes emotional profiling, price steering based on income inference, or personalised friction that slows access to protective choices. Therefore, unfair personalisation also includes personalised offers, discounts or prices based on profiling, inferred traits or situational signals such as location, device or purchasing behaviour. It also includes personalisation based on collected or derived traits that people neither have ever consented to provide nor they know or can know about. These practices rely on asymmetries of power. Traders hold the data, the predictions, and the models. People face an opaque system that anticipates their behaviour and adjusts their environment without their knowledge.

Profiling-based personalisation is unfair when it exploits vulnerability, alters visibility of options, prices or content without transparency, or relies on inferred traits that people cannot verify or contest. These systems operate largely out of sight, shaping rankings, recommendations and prices in ways individuals do not control. They can steer behaviour through emotional or behavioural signals, including in pricing practices such as drip pricing, device-based steering or dynamic adjustments that people cannot detect or challenge. **The result is structural harm to fundamental rights:** autonomy is weakened when environments adapt to vulnerability, data protection is undermined by uncontestable inferences, and equality is threatened when personalisation reproduces or amplifies exclusion. **Unfair personalisation is therefore not a neutral design choice but a systemic rights issue.**

Current EU law addresses only parts of this ecosystem. The GDPR limits profiling and bans processing of sensitive data unless strict conditions are met. While the DSA tackles recommender systems, but its obligations target large platforms only, and the DMA addresses ranking and self-preferencing for gatekeepers. None of these instruments prohibit unfair personalisation across all services, nor guarantee a neutral, non-personalised option by default. Similarly, these legislations do nott impose a general duty to prove that any personalisation respects autonomy, equality, and data protection.

EDRi's key recommendations

The DFA must close this gap by introducing clear obligations.

1. Prohibit personalisation based on sensitive or inferred traits

Unfair personalisation is built on profiling, which informs design choices and allows interfaces, prices or pathways to be adjusted in ways people cannot see or control. Traders adjust prices, discounts and fees using signals that people cannot detect or influence. This leads to unequal treatment and undermines the right to data protection. **Consumer law should prohibit personalised pricing based on profiling or inferred traits, and should ban device-, OS- or browser-based steering, unless it can be objectively justified.** It should require the total price to be shown upfront and ban drip pricing and dynamic price increases once an item has been added in the basket. It should restrict countdown timers, scarcity claims and vague reference prices that distort decisions or force people into rushed purchases. Where any form of price personalisation is permitted, **people must be able to disable it easily and access a non-personalised price without disadvantage.**

But unfair personalisation is not limited to pricing. The obligations must be broader. **The UCPD should prohibit commercial practices that exploit protected characteristics, inferred traits or situational vulnerability to steer decisions.** Using signals of fatigue, distress or financial pressure to shape content, prices or pathways should be treated as unfair personalisation. No service should adjust content or pathways based on health, sexuality, religious belief, political opinion, or traits inferred from behaviour. These inferences often fall within the GDPR rules on sensitive data. Using them to personalise experiences conflicts with EU fundamental rights and undermines the logic of data protection.

Advertising based on tracking and profiling uses the same system of cross-context data collection and sensitive inference. Large-scale behavioural advertising normalises surveillance, exploits situations of vulnerability and reinforces discrimination. **Consumer law should prohibit advertising models that rely on unlawful tracking or profiling, reinforcing GDPR's limits, while clearly preserving the lawfulness of contextual advertising that does not rely on personal data or profiling.** Contextual advertising that does not rely on individual-level identifiers remains compatible with this approach and avoids pressure on consent. This aligns consumer law with the Charter and with existing prohibitions on tracking-based advertising to minors.

2. Guarantee a functional non-personalised default

The DFA should require a fully-functional, non-personalised default mode of use where profiling materially affects how people access services, see content or offers, are priced, or exercise their data protection and equality rights, in line with GDPR requirements for freely given consent. This would preserve freely-given consent and reflect existing GDPR requirements. **Non-personalised modes should guarantee full functionality**. Refusing personalisation must never reduce access, visibility or usability. People should have full access to functionality without being profiled. This protects autonomy and reduces pressure. It would also support GDPR compliance by limiting situations in which traders try to justify profiling under claims of legitimate interest.

Personalisation should be opt-in. People must actively and knowingly choose to receive personalised content and have clear visibility of, and meaningful control over, the criteria and purposes by which personalisation operates. **Consent must be unbundled**, meaning that access to a service or its core features cannot be made conditional on agreeing to profiling or data use that is not strictly necessary. Refusing personalisation must not reduce access or degrade the service. This will restore meaningful choice and align consumer law with data protection law.

3. Prohibit tracking-based advertising models

Both the GDPR and the ePrivacy Directive already prohibit covert enrichment, which is defined assecretly adding extra data to a profile by pulling information from elsewhere, without people realising it is happening, as well as most forms of cross-context tracking. **The DFA should require consumer law enforcement to act in alignment with these prohibitions, without creating new legal bases.** Digital services gather vast amounts of data from browsing history, app activity, location patterns, and device signals. They merge these streams to infer sensitive traits. These practices create profiles that go far beyond people's expectations. **A general ban on covert or cross context data use is essential to stop profiling that violates data protection and fundamental rights.**

TABLE 11.Unfair personalisation: prohibited and conditional practices

Personalisation practice	Recommended legal status	Reason
Personalisation based on sensitive or inferred traits, including pricing, access and visibility	Prohibited	Always exploitative and discriminatory
Personalisation exploiting distress, fatigue or addiction or financial pressure	Prohibited	Targets situational vulnerability
Profiling-based steering of consent, prices, content or pathways	Prohibited	Circumvents the GDPR and autonomy safeguards
Opt-in personalisation with a fully functional non-personalised default	Permitted with safeguards	Respects autonomy and freely given consent
Contextual personalisation or advertising without tracking or profiling	Permitted	Does not rely on surveillance or structural manipulation

4. Impose a burden of proof for personalisation

Traders should be required to provide proof for any personalisation. They should **show that personalisation is necessary, fair, and proportionate.** Similarly, They should demonstrate that it does not exploit vulnerability or produce unequal outcomes. This burden-shifting model reflects the reality that regulators and people cannot assess these systems without evidence. **The trader holds the model, the data, and the design power. They must justify their choices.**

5. Ensure transparency of optimisation logic

The DFA should **require purpose limitation and transparency for recommender system optimisation.** Traders should disclose the objectives of optimisation, the signals used and the criteria that shape ranking, filtering or recommendations. This will help regulators understand how influence operates and how design affects access to information.

The DFA should align with the GDPR. It should not normalise unlawful profiling or expand the use of legitimate interest for profiling, training or enrichment. Personalisation must not bypass data protection law. **The DFA must strengthen, not weaken, existing protections.**

Unfair personalisation mechanisms shape behaviour at a structural level. They create unequal pathways, distort consent, and weaken autonomy. They rely on sensitive or inferred traits that people never agreed to share. The DFA **must address these practices through clear bans, strict defaults, and strong accountability for traders, in line with algorithmic justice**. A rights-centred framework is essential to protect autonomy, equality, and data protection in environments built around prediction.

7. BREAKING SILOS: COORDINATED, CROSS-REGULATORY ENFORCEMENT

Deceptive design, addictive architecture, and unfair personalisation are governed across different legal regimes. These issues affect autonomy, equality, and other fundamental rights. They also create consumer harm and distort competition. **No single authority can address these harms alone. Digital systems operate holistically, so enforcement must do so holistically too.** Otherwise, fragmented oversight leaves structural harms untouched.

Consumer law enforcement currently suffers from serious constraints. The system is decentralised. It relies on national authorities with limited resources and narrow mandates. Many authorities focus on individual cases of deception rather than optimisation systems that influence behaviour at scale. They often lack access to internal data, or design documentation. They also face slow processes, burdensome evidentiary requirements, and limited tools with which to address real-time or personalised manipulation. **This makes consumer law enforcement slow, reactive and easy to circumvent.**

Today, regulators work in parallel, in isolation from one another, without shared tools or shared evidence. Consumer protection authorities assess deceptive practices, data protection authorities assess profiling and consent, competition authorities assess market power, and Digital Services Coordinators assess systemic risks on platforms. While these and other regulators face different parts of the same system, they do not see the full picture. This allows traders to shift arguments, minimise responsibility, and avoid meaningful scrutiny.

This fragmentation enables harmful practices persist. A service under consumer scrutiny may frame a practice as a data issue, under data protection scrutiny may present it as a design issue, and under competition scrutiny may argue that its influence mechanisms are neutral features. **This legal switching creates gaps in protection.** It weakens enforcement and delays remedies, leaving people exposed to repeated rights violations across multiple services.

EDRi's key recommendations

The DFA must address this problem by implementing structural coordination measures. Regulators need shared standards and shared access to evidence. To meaningfully operate, they need the same baseline understanding of design systems, profiling logic, and attention capture mechanisms. The DFA should create obligations connecting consumer, data protection, competition, and digital services authorities, as well as potentially other regulators.

1. Duty of cooperation across authorities

The DFA should **introduce a duty of cooperation across all relevant authorities.** This duty should require active coordination on cases that involve manipulative design or unfair personalisation. Authorities should not work in isolation when the harms are systemic.

The Consumer Protection Cooperation (CPC) Regulation should be **strengthened to support coordinated investigations, evidence sharing and effective enforcement against cross-border manipulation.** CPC authorities must work seamlessly with data protection, competition, media and digital services regulators. To this aim, a dedicated cooperation mechanism is needed to facilitate the sharing evidence, the launching joint actions and the prevention of gaps between networks. Therefore, the DFA should be accompanied by a strong CPC revision that reinforces national authorities, grants the Commission direct enforcement powers in cross-border digital cases, and enables joint investigations into unfair design and personalisation across Member States.

2. Shared evidence and transparency obligations

Regulators across the board must share key evidence. This includes design transparency logs, profiling documentation, risk assessments, data protection impact assessments, recommender system documentation, and fairness testing results. Much of this material is already produced by traders . Regulators need access to it across regimes. Sharing evidence reduces duplication and closes loopholes, and it also strengthens the ability of authorities to detect patterns that violate rights.

The DFA should **empower regulators with meaningful access to internal optimisation data**. Authorities should be able to inspect system objectives, model inputs, optimisation criteria and experiment outcomes. As influence systems operate at scale, regulators need access to the internal logic to understand how an interface or recommender system shapes behaviour.

3. System-level assessment of influence systems

Enforcement must focus on system logic, not isolated patterns. Manipulation emerges from optimisation goals, data inputs and experimental results. These elements drive how design evolves, how prompts are targeted and how personalisation adapts to behaviour. When evaluating fairness, regulators should assess system-level optimisation choices, including objectives, data inputs and experiment design. This must include the objectives that models optimise for, the data used to personalise interfaces, and the experiments that shape behavioural outcomes. **A system logic approach allows regulators to detect harm even when no single feature appears unlawful. It also prevents traders from hiding influence** behind self-learning systems that adapt faster than case-by-case enforcement.

4. Composite and coordinated investigations

The CPC Regulation should also support composite investigations, enabling regulators to run joint cases when a practice raises issues across consumer law, data protection, competition or digital services law, among potentially others. Harmful design systems operate exactly at these intersections. **Composite investigations would allow regulators to issue coherent remedies that address the whole system, not isolated symptoms.**

The DFA should equip authorities with pattern-based analytical tools to identify structural manipulation across services and over time, rather than assessing isolated interface elements in isolation. **Regulators should assess indicators such as friction asymmetry, emotional steering, and structural nudging.** These indicators reveal how influence operates across systems. and help authorities identifying harm that is invisible at the level of individual features.

Procedures and timelines should be aligned. Currently, investigations progress at different speeds across regimes, with traders targeting the slowest or least equipped authority. A coordinated framework and timeline would reduce this imbalance, prevent delays and strengthen rights under the Charter. **Autonomy, dignity, equality and data protection cannot be protected when regulators work in silos.** Structural oversight is needed to confront structural harm. Such coordinated enforcement protects legitimate economic actors, as companies that refrain from manipulative practices suffer when enforcement is inconsistent. They face competitors who deploy harmful design without facing any consequences. A coordinated model restores fairness andensures that traders who respect rights do not operate at a disadvantage.

5. Deterrence, penalties and effective redress

Deterrence and remedy must reflect systemic harm, and so penalties should match the scale of manipulation. Penalties should be effective, proportionate and dissuasive across Member States. A harmonised minimum level of fines would strengthen deterrence for systemic manipulation. **Remedies should include design reconfiguration**, not only fines. Services must be required to remove harmful optimisation logic, reduce behavioural triggers or change interface flows when these patterns produce unfair outcomes.

The legal framework for collective and cross-border redress should **ensure that courts can apply the law of the forum when manipulation cases span across multiple Member States.** The legal framework for collective and cross-border redress should **ensure that cross-border manipulation cases are not undermined by complex choice-of-law fragmentation under Rome I and Rome II**. The interaction between the DFA and the existing private international law framework should be assessed to ensure that collective actions remain effective and do not stall on procedural disputes over applicable law. Where necessary, targeted adjustments to preserve effective redress in cross-border manipulation cases should be considered. In this way, collective redress remains effective and does not stall on complex choice-of-law disputes. This would prevent procedural obstacles and ensure that people harmed by digital manipulation do not receive unequal protection depending on where the trader is established.

The digital environment is shaped by interconnected systems of influence. Enforcement must reflect this reality. **Coordination is not administrative convenience, it is the only way to protect people from structural harm.** The DFA must build a model where EU regulators work together, share evidence, and act on the full ecosystem of design, personalisation, and profiling.

TABLE 12. From fragmented oversight to coordinated enforcement

Current enforcement reality	Enforcement under the DFA
Parallel investigations with limited scope	Joint or mutually informed assessments
Different legal tests applied in isolation	Shared fairness benchmark across regimes
Reactive intervention after harm occurs	Preventive intervention against harmful design
High evidentiary burden on authorities	Design-level accountability on traders

The DFA is a chance to confront a simple reality: **today's digital environments are engineered to influence behaviour at scale, with direct implications for digital rights,** including autonomy, equality, access to information and the fundamental rights to data protection and privacy. Fragmented and insufficiently modernised consumer rules and case-by-case enforcement are not enough to address systems built to manipulate, extract and optimise against people's interests. Therefore, a **rights-based DFA must focus on clear prohibitions, strong defaults and enforceable responsibilities** for those who design and deploy these systems. By anchoring consumer law in digital rights, strengthening coordination between regulators, and targeting business models that depend on behavioural manipulation, **the DFA can restore meaningful agency, protect people using all digital services and ensure that digital rights are upheld in practice, not only on paper.**

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights