COMMENTS TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DIGITAL FAIRNESS ACT

SUBMITTED BY CONSUMER ASSOCIATION IUS OMNIBUS

I. IUS OMNIBUS

Ius Omnibus (Ius), with registered office at Second Home Lisboa, Mercado da Ribeira, Av. 24 de Julho, 1200-479 Lisbon, Portugal, is a non-profit association, created in March 2020, with the aim of promoting and defending the rights and interests of consumers in the European Union. It is a consumer protection association registered and recognised by the Portuguese Government and the European Commission as a qualified entity under Directive (EU) 2020/1828, which has filed several class actions in the field of consumer protection.

Ius' interest in participating in this public consultation on the Digital Fairness Act (DFA) stems from its commitment to the effective defence of consumer rights in the digital environment. As an association dedicated to promoting fair and undistorted competition, as well as the collective protection of consumer interests, Ius considers it essential that this new legislation guarantees a digital ecosystem that is transparent, equitable and respectful of the fundamental rights of European citizens.

Ius has found that unfair online commercial practices – including the use of misleading interfaces, covert advertising on social media, design strategies, and manipulation based on personal data – erode consumer confidence and exacerbate information asymmetries between platforms and users. These practices have a particularly serious impact on minors and vulnerable consumers, who require enhanced protection. The erosion of trust in markets is not only a matter that affects consumer welfare but is directly related to the strength of markets and their ability to be innovative and competitive. That is why the implications of a fair and equitable digital environment transcend the immediate objectives of consumer protection.

Ius has demonstrated a consistent commitment to citizen participation and transparent governance through its active involvement in numerous public consultation processes at both national and European level. One example is its participation in the public consultation on the revision of the Digital Market Act and the submission of comments and proposals

aimed at strengthening transparency and fairness in digital markets, with a particular focus on the role of large online platforms, interoperability and the protection of effective competition.

II. Public consultation

The European Commission has launched a public consultation on the future Digital Fairness Act. The main objective of the Digital Fairness Act (DFA) is to ensure that digital commercial practices are transparent, fair and understandable to users, while preserving an environment conducive to innovation and business competitiveness. In a context characterised by the growing complexity of algorithms, price personalisation, the use of persuasive interfaces, and the monetisation of personal data, it is essential to adapt traditional legal instruments to ensure effective consumer protection and fair competition conditions.

The public consultation launched by the Commission represents a decisive opportunity to review and modernise the regulatory framework for commercial practices in the digital environment, complementing existing instruments such as the Unfair Commercial Practices Directive[1] (Directive 2005/29/EC), The *Digital Services Act*[2] (DSA) and the Artificial Intelligence Regulation[3] . In this regard, the DFA is conceived as the pillar that will enable a dynamic balance between consumer protection, technological innovation and market fairness.

Ius' participation is essential to convey to the Commission the experience of consumers with digital practices and to promote an approach that prioritises damage prevention and accountability on the part of operators.

As a preliminary point, we would like to emphasize that we consider it essential that the regulatory instrument through which the approval of the rule is conveyed be a regulation. There are several reasons to believe that this would be a better alternative to a directive. Firstly, because of the delays that often characterise the approval of directives. The necessary transposition of directives by Member States usually contributes to long periods of delay in their implementation. In contrast, the direct effectiveness of regulations allows for more immediate application, which means that the regulations can be implemented in a shorter

[1] DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council.

[2] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC.

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

period. In addition, a regulation allows for a much more harmonised application of the measure.

III. Comments

The DFA comes at a key moment in the maturity of the Regulation of European digital single space, characterised by the expansion of e-commerce, the platform economy and the intensive use of algorithms and personal data to model consumer behaviour.

Although the European Union has already adopted a comprehensive body of digital regulations, such as the DSA, the *Digital Markets Act*[4] (DMA) and the *Data Act*[5] –these instruments focus primarily on competition, the transparency of intermediaries and access to data, but do not directly address fairness and consumer protection from the perspective of digital commercial practices.

The DFA proposes updating these regulations to the new digital ecosystem.

In this regard, the "*Fitness Check on EU Consumer Law on Digital* Fairness"[6] prepared by the Commission in 2024 reveals that the Directives implemented, although still relevant, were designed before the large-scale rise of digital markets[7]. Although they have been applied in the digital environment, they lack the specificity necessary to address some of the emerging issues brought about by digitalisation.

For example, although Directive 2005/29/EC on unfair commercial practices provides a general framework and could encompass new practices such as dark patterns and personalised advertising. However, these digital practices are often more sophisticated and manipulate consumers in more subtle and complex ways than traditional offline methods.

The underenforcement of unfair practices, along with a legal terminology too loose and broad for specific conducts make it advisable to have a regulation of its own and avoid bundling a wide array of practices under the same infringement. The DFA therefore seeks to address the persistent shortcomings in the digital field which, despite attempts, the Commission has not yet managed to resolve.

Specifically, the weaknesses identified by the European Commission in the report "*Fitness Check on EU Consumer Law on Digital Fairness*" in the regulations currently in force are:

---

[4] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828.

[5] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

[6] SWD(2024) 230 final of 3 October 2024, available at the following link: 707d7404-78e5-4aef-acfa-82b4cf639f55_en.

[7] Nikiforov, Liubomir. *Digital Fairness Act: If and How?* Brussels Privacy Hub, October 2024. https://brusselsprivacyhub.com/wp-content/uploads/2024/11/Digital-Fairness-Act-If-and-How-Liubomir-Nikiforov.pdf.

- Lack of explicit coverage of new digital practices, such as dark patterns, personalised marketing or algorithmic manipulation.
- Difficulties in ensuring uniform and effective application and enforcement in all Member States.
- Regulatory fragmentation and national divergences in the transposition and interpretation of the Directives and other instruments in place.
- Limited practical effectiveness of certain rights, due to lack of awareness or lack of agile complaint mechanisms.
- Extensive information requirements that may be difficult for the average consumer to understand.
- Insufficient capacity of national authorities to monitor and sanction in the digital environment.

In conclusion, the aim is to ensure that consumer rights remain enforceable regardless of the business model used or the technological design. In other words, to create a coherent legal framework that equally guarantees the rules for the protection of digital and analogue consumers.

These concerns are not merely theoretical, but are reflected in our daily work as a consumer organisation: coordinating with public authorities, ensuring access to justice for these conducts, and the availability of adequate resources or funding remain key factors for the proper enforcement of the law and the effective defence of consumer rights.

In this regard, and continuing with the interest expressed in the Consumer Agenda public consultation, we present our comments on possible improvements to the DFA with the aim of better securing digital environments.

Ius Omnibus believes that the DFA should serve to promote digital justice. To this end, it is essential to integrate mechanisms for assessing the impact of algorithmic practices and to strengthen the capacity for sanctions and coordinated supervision between national and European authorities.

1. REGULATORY IMPROVEMENT FOR DARK PATTERNS

The proliferation of *dark patterns* –digital interface design techniques intended to manipulate or influence consumer decisions– poses a significant regulatory challenge in the field of consumer law, competition law and data protection. According to the Commission's estimates, the economic damage suffered by consumers in the digital space has almost doubled since 2017. At the same time, there is a lack of clear legal rules and consistent

enforcement in Member States, creating legal uncertainty for both consumers, consumer organisations, and businesses[8] .

The aforementioned damage must be put into perspective with the large profits made by offending companies at the expense of consumers. It is precisely this type of distribution that makes it necessary to have a rule that focuses on fairness and is aware that, although the damage caused may not be serious, this does not justify promoting a business model that in no way benefits the consumer, as this, as explained above, has negative medium- to long-term effects on the market by affecting confidence and, ultimately, competitiveness.

Although the European Union already has an extensive legal framework addressing misleading and unfair practices, the absence of a uniform definition of *dark patterns* creates legal uncertainty and hinders their effective enforcement. This vague definition is also consistently challenged by defendants, which adds yet another barrier to achieving legal certainty over the terminology of dark patterns.

The future DFA represents a key opportunity to remedy this situation and establish coherent, cross-cutting and effective regulation that specifically addresses *dark patterns*. However, its success will depend on its ability to integrate the various existing provisions on consumer protection, e-commerce, data protection, competition, and digital design.

Currently, the phenomenon of *dark patterns* is partially covered by several European regulations. Directive 2005/29/EC prohibits misleading or aggressive practices in business-to-consumer relations, and its application has made it possible to sanction certain online behaviours that distort the user's decision. However, this Directive was designed for an analogue environment and focuses on observable commercial behaviour, without addressing digital design mechanisms that mislead or hinder the exercise of rights. The legal systems of some Member States allow for the sanctioning of these practices under current legislation, particularly in Germany, whose case law is a good reflection of this[9]. However, this cannot be extrapolated to the legal systems of other Member States, which are characterised by much more fragmented regulation.

For its part, the General Data Protection Regulation[10] (GDPR) imposes the principle of free and transparent consent, which prohibits the use of interfaces that pressure or manipulate users into accepting the processing of their data. Although the GDPR is an effective tool in this area, its application is limited to cases where personal data is processed, leaving out many purely commercial manipulative strategies.

From the perspective of personal data collection, special attention must be paid to the principle of minimisation set in Article 5(1)(c) GDPR, so that users only have to provide the

[8] Heuking Kühn Lüer Wojtek. "New plans from the EU Commission: The Digital Fairness Act." *Heuking Kühn Lüer Wojtek,* 23 May 2025. https://www.heuking.de/en/news-events/newsletter-articles/detail/new-plans-from-the-eu-commission-the-digital-fairness-act.html.

[9] Regional Court Bochum, judgment of 10 September 2015 – 14 O 55/15.

[10] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

data that is necessary for the functionality or digital service to be provided. It is common for registration on an app or website to require certain personal data, just as apps or websites may offer different service packages. Although each service requires certain user data in order to be provided, many websites or platforms collect all possible personal data by default, so that the design itself allows for much more data to be collected than the user would have provided if the collection had been in accordance with the principle of data minimisation. We therefore propose that the DFA contain an express provision for this type of practice, which will also contribute to more effective public enforcement of this essential principle of data protection by the various national and European agencies.

Directive 2011/83/EU[11] imposes pre-contractual information and transparency obligations on distance contracts. Certain practices, such as making it difficult to cancel a subscription or hiding information about the right of withdrawal – the so-called "*roach* motel" – may be considered infringements of the Directive. However, this directive does not expressly refer to *dark patterns* or consider their systematic nature in digital environments.

Other regulatory instruments, the DSA and the DMA, referred to above, incorporate more specific prohibitions. Article 25 of the DSA explicitly prohibits misleading designs that limit or distort the user's ability to make free and informed decisions, but its application is restricted to online platforms, not other online actors. The DMA, for its part, imposes similar obligations on *gatekeepers,* particularly with regard to the withdrawal of consent, although it only affects the small number of operators which have been designated as gatekeepers.

The common diagnosis is clear: current regulation is fragmented, sectoral and lacking in systematic coherence. First, the absence of a unified legal definition of the concept of *dark patterns* causes legal uncertainty. Each regulation approaches it from a different angle—data protection, commercial practices, contractual transparency or platform regulation—without establishing a common category or objective identification criteria. Secondly, the difficulty of proving intent is a major obstacle. *Dark patterns* are designed to appear functional or neutral, making it difficult to prove that a practice was deliberately designed to manipulate consumers. Finally, the practical application of the rules lacks traceability: national authorities do not record whether the enforcement measures adopted specifically address dark patterns, which makes it impossible to assess the effectiveness of public policies and enforcement mechanisms[12].

Given this scenario, the DFA should be configured as a horizontal instrument that unifies criteria and strengthens the capacity of authorities to prevent and sanction these practices. A first necessary step would be to introduce a legal definition of *dark patterns* that encompasses both their intentional dimension and their effect on consumer autonomy. As these behaviours normally occur at the European level, if not higher, it is advisable to have a harmonised definition of the term to avoid disparity in criteria and "standards of deception" in different jurisdictions. Litigation arising from dark patterns will take place within a Member

[11] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.

[12] European Parliamentary Research Service. Regulating Dark Patterns in the EU: Towards Digital Fairness. Brussels: European Parliament, 2025.

State or will reach the Court of Justice of the European Union (CJEU) through a preliminary ruling. It is therefore advisable to try to minimise the legal uncertainty and insecurity that a vague definition of the term may entail.

It could be understood as any digital interface design or structure deliberately conceived to distort, manipulate or limit the user's freedom of choice, causing a result that the user would not have consciously and voluntarily chosen.

It would also be advisable to classify *dark patterns* into different categories according to their mechanism of action. These could include deceptive practices, which manipulate information through ambiguous language or omissions; coercive practices, which create urgency or psychological pressure; obstructive practices, which make it difficult to exit or cancel a service; covert practices, which introduce unauthorised costs or elements; and emotional practices, which appeal to guilt or shame to induce a decision. This typology would facilitate the identification of behaviours and allow for more proportionate regulatory treatment.

Likewise, the DFA should provide for the development of common technical guidelines by the European Commission and the competent authorities to define objective indicators for detecting, measuring and documenting the existence of dark *patterns*. These guidelines will serve as standardisation requirements for software developers as well as for digital users, who will be better aware of which practices are acceptable, and which ones surpass such threshold.

At the same time, the DFA should establish specific responsible design obligations, ensuring that interfaces comply with principles of neutrality, clarity and information symmetry. It would be advisable to require large platforms to carry out ethical design impact assessments, similar to data protection impact assessments. In terms of sanctions, fines should be calculated not only on the basis of formal non-compliance, but also on the economic benefit obtained through the manipulative practice. In addition, a system of shared responsibility between the trader, the interface designer and the developers involved in its implementation should be provided for.

From an institutional point of view, it is proposed that a European *Dark Patterns* Observatory be set up to collect, analyse, and disseminate information on cases detected in Member States, as well as to coordinate the actions of national authorities. It would also be essential to strengthen cooperation between data protection agencies, consumer authorities and competition authorities, given that the effects of these practices transcend the traditional boundaries of each regulatory area.

Finally, the DFA should promote transparency and digital education. Requiring traders to publish regular reports on design criteria and their effects on the user experience would contribute to greater accountability. At the same time, the promotion of digital literacy programs would enable consumers to recognize and resist the most common manipulative strategies.

In conclusion, the DFA represents a decisive opportunity to unify the legal treatment of *dark patterns* and strengthen consumer protection in the European digital environment. The current regulatory mosaic offers partial and fragmented protection, which is insufficient in the face of the sophistication of contemporary manipulation techniques. Truly effective regulation must combine a clear and flexible legal definition, ethical design prevention mechanisms, presumptions of intent in cases of structural bias, and effective cooperation between competent authorities. Only through this comprehensive and coordinated approach can the European Union ensure digital fairness, strengthen real consumer autonomy, and promote a transparent, ethical, and fair technological environment.

2. STRENGTHENING CONSUMER PROTECTION IN ONLINE ECOSYSTEMS

Directive 93/13/EEC[13] was conceived in a pre-digital context in which contracts were concluded using physical documents and relatively transparent negotiations. Its structure and purpose respond to a logic of *ex post* protection, focused on the nullity or inapplicability of unfair terms detected in adhesion contracts. However, technological developments have shifted the contractual reality towards opaque digital environments, characterized by automated contracting, one-click acceptance and the integration of complex clauses into lengthy electronic texts that consumers rarely read or understand.

Even from a pre-contractual point of view, consumers are often unprotected in digital environments due to the wide variety of services on offer, where free versions of these services, or those with more limited functionality that are less expensive or offer less data protection, are difficult to find information about and access.

Furthermore, many of the practices observed do not relate to a misunderstanding of the contractual terms, but rather to the difficulty of enforcing them. For example, a user who receives advertising as part of a newsletter may be aware of their right to opt out of receiving such commercial communications. However, it can be confusing and difficult for consumers to cancel a subscription or unsubscribe from a service.

In this context, the proposal for a DFA is an attempt to update consumer protection instruments to new forms of electronic contracting. The DFA aims to reinforce the principles of transparency, legibility and accessibility, already implicitly included in Article 5 of Directive 93/13/EEC and Article 12 of the GDPR, giving them an operational and verifiable dimension in the digital environment.

The proposal is in line with the principles of '*privacy by* design' and '*information by* design', enshrined in Articles 25 and 12 of the GDPR, according to which user information and protection obligations must be integrated from the design stage of services. Thus, the DFA aims to transfer this logic to the contractual sphere, so that digital contracts are understandable from their conception, and not only reviewable in the event of litigation.

[13] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

However, the proposal raises several interpretative and practical challenges:

Firstly, the objective determination of contractual "*comprehensibility*".

Although the principle of transparency is already present in the European legal acquis, its effective application in digital environments is problematic. Article 5 of Directive 93/13/EEC requires that clauses be drafted "*in plain and intelligible language*", and the CJEU, in cases such as *C-26/13, Kásler and Káslerné Rábai*[14] or *C-96/14, Van Hove*[15] , has interpreted this requirement not only in linguistic terms, but also in material terms: the consumer must understand the economic and legal consequences of the clause.

However, transferring this requirement to the digital sphere implies the need for technical evaluation criteria. It is essential to develop standardised methodologies, based on readability indicators, user tests or clear language models, to verify the comprehensibility of contracts before they are deployed. Otherwise, the obligation of clarity could degenerate into a purely formal requirement with no practical effect.

Secondly, there is the risk of formalism and symbolic compliance.

One of the main risks of DFA is the excessive formalization of transparency requirements. Experience shows that linguistic simplification or reduction in length does not guarantee actual comprehension. Consequently, it would be necessary to introduce empirical validation mechanisms – for example, comprehension audits or 'clear contract' certifications – supervised by competent authorities or accredited entities, in accordance with the principles of effectiveness and proportionality set out in Article 5 TEU.

Thirdly, with regard to the responsibility of intermediary platforms.

The proposal reopens the debate on the responsibility of digital intermediaries. Under the DSA, platforms already assume duties of diligence in content moderation and transparency. Extending this logic to the contractual sphere would imply recognizing their joint responsibility for consumer protection, especially when they act as facilitators of contracting or indirect beneficiaries of contractual content.

In this regard, we must highlight and take advantage of the position of the trusted flaggers referred to in the DSA, who are trained to carry out these enhanced supervision tasks on access to services and the conditions under which consumers enter into contracts.

In line with this, a regime of shared or *subsidiary* liability could be established, for example, whereby platforms would be required to verify that the contracts hosted comply with the transparency standards set out in the DFA, under threat of administrative sanctions in the event of non-compliance. Such a mechanism would reinforce the systemic coherence of European digital law by integrating contractual protection with the platform governance provided for in the DSA.

[14] Judgment of the CJEU of 30 April 2014, ECLI:EU:C:2014:282.
[15] Judgment of the CJEU of 23 April 2015, ECLI:EU: C:2015:262.

In conclusion, the DFA constitutes a significant step forward in the evolution of European consumer law, by transferring the classic principles of transparency and fairness to digital environments. However, its effectiveness will depend on its technical implementation and its articulation with the rest of the regulatory acquis. To ensure that the regulation does not remain a programmatic mandate, it will be necessary to establish verifiable comprehensibility criteria, certification mechanisms and a clear regime of platform liability. Only in this way can the essential objective of European legislation be achieved: to guarantee real and effective protection for digital consumers, in accordance with Article 38 of the Charter of Fundamental Rights of the European Union and Article 169 of the TFEU.

3. STRENGTHENING THE PROTECTION OF THE AVERAGE CONSUMER

The classic notion of the 'average consumer', consolidated by the case law of the CJEU – particularly in cases such as *C-210/96, Gut Springenheide and Tusky*[16] and *C-220/98, Estée Lauder*[17] – is defined as a reasonably well-informed, observant and circumspect person, taking into account social, cultural, and linguistic factors. This standard, which has been used as an interpretative standard in matters of unfair terms, misleading advertising and unfair commercial practices, is based on a homogeneous conception of the consumer, understood as an abstract and uniform type.

However, this construct is insufficient in the contemporary digital ecosystem, where consumer interactions are highly personalised through algorithmic profiling and recommendation systems. Digital platforms use large volumes of behavioural data to tailor prices, offers and advertising content to each user, creating an environment of dynamic information asymmetry and, in many cases, exploiting specific psychological or cognitive vulnerabilities. This phenomenon goes beyond the protective framework designed for a generic average consumer, as the impact is no longer directed at a uniform audience, but at segments individualized according to their behaviour or susceptibility.

Against this backdrop, the DFA introduces a reinforced category of protection for vulnerable consumers, advancing along the lines already outlined by Directive (EU) 2019/2161[18] and by Article 5(3) of Directive 2005/29/EC. The latter expressly recognizes the special protection of consumers who are "particularly vulnerable because of their age, credulity or mental or physical disability". The DFA expands and updates this notion, also incorporating people with low digital literacy, an emerging group whose vulnerability stems not from their intellectual capacity, but from their lack of technical skills to understand digital contracting, data processing and automated decision-making processes.

[16] Judgment of 16 July 1998, ECLI:EU: C:1998:369.
[17] Judgment of 13 January 2000, ECLI:EU:C:2000:8.
[18] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the improvement of the enforcement and modernization of Union consumer protection rules.

This is undoubtedly an ethically and socially significant advance, as it recognises that formal equality of online consumers does not imply material equality of opportunity or understanding. The proposal responds to the principle of digital solidarity and is in line with the mandate of Article 38 of the Charter of Fundamental Rights of the European Union, which requires a high level of consumer protection to be guaranteed. It can also be interpreted as a concrete expression of the principle of non-discrimination and protection of vulnerable groups, enshrined in Article 9 of the TFEU, which imposes on the Union the obligation to take into account social protection requirements in all its policies.

However, its practical implementation presents significant challenges:

A. Identifying vulnerable consumers.

Determining who is actually vulnerable in the digital environment is a complex task. The use of demographic categories (age, disability, digital literacy) can be problematic if it involves the collection or processing of sensitive personal data, in possible conflict with the principles of minimisation and purpose limitation in Article 5 of the GDPR. An automated application of the concept could even create a risk of stigmatization, where users are labelled as "vulnerable" based on classification algorithms. Therefore, the regulatory design must ensure that identification is carried out without violating the privacy or rights of the data subjects, probably through voluntary self-identification mechanisms, accessibility certifications or universal design requirements applicable to all users.

The case of younger people is particularly significant. Children, especially those of the so-called "Alpha" generation, are growing up in a digitalised society and incorporating these types of technologies from a very early age. On the one hand, this leads to a much higher degree of exposure as digital consumers, which increases the risk they face in quantitative terms. On the other hand, the digital environment is not unfamiliar to these children, so their vulnerability is mainly determined by their age, rather than by other factors that exacerbate their vulnerability.

For example, in the case of older people, the technological component is an added factor to a situation they might face as consumers in an analogue environment.

B. Specific protection measures.

The effectiveness of this enhanced protection will depend on the implementation of specific measures. These could include:

- The obligation to provide accessible and understandable interfaces, in line with digital accessibility standards (Directive (EU) 2016/2102[19] and the European Accessibility Act 2019/882[20]);

[19] DIRECTIVE (EU) 2016/2102 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies.
[20] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services.

- A ban on manipulative techniques or misleading design aimed at vulnerable users;
- Obligations to assess the impact on digital equity, analogous to data protection impact assessments (Art. 35 GDPR);
- These measures would transform digital consumer protection from a reactive model to a preventive and ethically designed one.

C. Compatibility with the principle of technological neutrality.

An additional risk lies in the potential tension with the principle of technological neutrality, enshrined in the Union's regulatory policy. If the regulations impose different obligations depending on the user profile or the technology used, this could introduce indirect discrimination or create legal uncertainty. The key will be to formulate a framework based on results rather than specific technologies, i.e. focused on ensuring equivalent levels of protection regardless of the technical medium or type of interface.

At Ius Omnibus, we promote innovation and technological advances, as we understand that they can improve the consumer experience and well-being. Technological neutrality should not be understood as a linear and stagnant technology accessible to all, but rather as a minimum margin in the rights and obligations of providers and users, in short, a level playing field from which to continue building.

D. Coherence with the European legal acquis.

Enhanced protection for vulnerable consumers must be integrated coherently with existing rules, in particular Directive 2005/29/EC, Directive 2011/83/EU and the DSA. Insufficient harmonisation could lead to regulatory overlaps or conflicts of interpretation, particularly in the distinction between unfair commercial practices and the exploitation of vulnerabilities.

Ultimately, the DFA represents a decisive step towards the humanization of digital law, recognizing that formal equality in electronic contracts does not equate to substantive fairness. However, its success will depend on the ability of the regulation to balance differentiated protection with respect for privacy, technological neutrality and regulatory proportionality. In this regard, the most significant challenge will be to design inclusive, non-invasive and technologically neutral protection mechanisms that translate the principles of fairness and transparency into concrete, verifiable and effective obligations for digital operators.

4. IMPROVING COMPETITIVENESS IN DIGITAL ECOSYSTEMS

The DFA aims to become a key regulatory instrument for balancing the relationship between consumers and digital operators, while also serving as a lever for sustainable competitiveness within the European digital single market. Its potential impact is not limited to strengthening user rights but could transform the very structure of competition in digital environments, including video games, e-commerce platforms and algorithmic services.

In today's digital economy, opaque business practices, price personalisation, manipulative interfaces and indiscriminate use of data create a profound information asymmetry between consumers and businesses. These dynamics not only undermine transparency but also distort competition by favouring those who operate without clear ethical or information standards. In this context, the DFA has the potential to restore trust and establish a common framework of digital fairness that benefits both users and businesses.

Even though the effects on fair competition may be an indirect result of ensuring digital fairness and there are other instruments tailored to promote competitiveness, such as the DMA and articles 101 and 102 TFEU, the DFA should acknowledge its potential effects on competition and the role it plays in the EU legal acquis.

First, the DFA could strengthen competitiveness through standardisation and interoperability. The standard should not only require transparency in algorithms and digital systems, but also promote open technical standards that facilitate interoperability between platforms and services. This would reduce technological dependence on large providers, expand opportunities for digital SMEs and independent developers, and enable true data and content portability. Interoperability, in addition to promoting fair competition, drives incremental innovation, as new players can build services on existing technologies without artificial barriers.

With regard to interoperability, we have already expressed our concern about ensuring interoperability in previous public consultations (DMA.100204 SP-APPLE-ARTICLE 6(7)[21]). Although this is a technical issue involving large technology companies such as Apple and developers who encounter barriers in the development of their projects, interoperability has important effects for consumers. Any restriction on supply imposed for no other reason than to maintain a dominant position ultimately indirectly controls the content offered and the consumer's freedom to decide freely. Therefore, another area that should be included in the DFA regulatory framework is interoperability.

Secondly, the DFA could improve its competitive impact by incorporating mechanisms for regulatory cooperation and supervised self-regulation. Instead of focusing exclusively on sanctions, the regulation could provide for cooperative compliance systems – for example, sectoral codes of conduct, transparency certifications or digital trust seals – that recognise and reward companies that go beyond the minimum obligations. This approach, already successfully employed in the areas of data protection and cybersecurity, would transform regulatory compliance into a reputational and competitive advantage, encouraging companies to invest in responsible practices not as a burden, but as added value.

In turn, the DFA can act as a stimulus for responsible innovation. By establishing standards of transparency and fairness, the regulation encourages the development of digital products and services designed from the outset with criteria of trust and respect for the user. This approach – known as "compliance by design" – turns ethics and consumer protection into positive differentiating factors. Thus, European companies compete not only on price or

[21] Contribution submitted by Ius Omnibus available here.

data volume, but also on quality, transparency and sustainability, strengthening the global positioning of the European digital ecosystem.

The future regulation may also help to reduce litigation costs and regulatory fragmentation between Member States. By harmonising the rules on unfair practices, transparency and the burden of proof, the DFA eliminates the need to adapt compliance strategies on a country-by-country basis, facilitating the expansion of digital companies within the Union. Furthermore, incorporating procedural mechanisms such as evidentiary presumptions, technical documentation obligations, and proportional access to evidence will reduce legal disputes arising from technological opacity, creating a more efficient and competitive environment.

Example: Responsible Design in Video Games

The DFA could have a decisive impact on the video game industry. For instance, the obligation to display prices in real currency, to publish the probability of random rewards, and to offer options to deactivate payment or random features not only protect consumers but also fosters fairer competition based on transparency and design quality. Developers who adopt more ethical models will likely see stronger reputation and player loyalty, while manipulative practices will gradually disappear from the market. In this sense, clear information and respect for the player become key elements of competitive advantage.

Furthermore, the DFA's approach promotes fair competition in which consumer trust becomes an economic asset. Companies that comply with the principles of digital fairness and respect for users will not only avoid penalties, but will also gain legitimacy and positioning over less transparent competitors. In the long term, this strengthens the reputation of the European digital market and attracts foreign investment by offering a stable and reliable regulatory environment.

From a strategic brand positioning perspective within the European Union, the promotion of these values by companies can represent added value and a fundamental pillar of corporate culture, which values consumer welfare and seeks to make it an essential starting point in its innovation process. If this message is internalised by companies in the sector and by civil society, it can have a significant impact on digital consumption and innovation and investment in this industry within the EU.

Finally, by establishing itself as a global regulatory model, the DFA can project the influence of the European Union beyond its borders. Just as the GDPR became an international privacy standard, the DFA can establish itself as a benchmark for transparency, fairness and digital responsibility. This regulatory leadership not only protects consumers but also gives European companies an international competitive advantage by operating under a framework recognized for its reliability and commitment to technological sustainability.

In short, the DFA should not be understood solely as a consumer protection law, but as a tool for economic policy and competitive strengthening. By building trust, levelling the

competitive playing field, encouraging ethical innovation, reducing regulatory costs and projecting a model of digital fairness to the rest of the world, the DFA can place the European Union at the forefront of a new economic paradigm.

5. IMPLEMENTATION AND ENFORCEMENT

The current system for enforcing consumer law in the European Union relies heavily on Regulation (EU) 2017/2394 (known as UCPD)[22],which constitutes the cornerstone of the regulatory framework governing unfair commercial practices in the Member States and it establishes the Consumer Protection Cooperation Network. This network seeks to ensure cooperation between national authorities responsible for consumer protection, particularly in relation to cross-border infringements. However, its structure – based on voluntary administrative cooperation, mutual notification and reciprocal assistance – has proved insufficient to tackle the abusive practices of global digital platforms, whose scale and technological complexity exceed the capacity of national authorities to take action. Thus, while the UCPD provides a comprehensive general framework for these behaviours, it lacks the required specificity to address complex and subtle conducts taking place in the digital space.

For instance, take dynamic algorithmic pricing, a conduct that can well be considered as unfair. This pricing policy is unfair under the UCPD, however, none of the articles there in account for a proper labelling of the conduct. Fairness, and thus, justice for consumers and users requires of a regulation able to encapsulate and denominate unlawful behaviours more concretely.

The difficulties lie, among other factors, in the lack of procedural harmonisation, the asymmetry of technical resources between Member States, and the dependence on intergovernmental cooperation. This creates a risk of fragmentation in the application of European consumer law, contrary to the principle of effectiveness and uniformity of Union law. In fact, cooperation procedures for consumer protection are often slow, lack adequate forensic tools to audit algorithms or segmentation systems, and depend on the goodwill of digital operators, many of whom are located outside the EU or under complex corporate structures.

Aware of these limitations, the European institutions, through the DFA, propose a substantial strengthening of the *enforcement* framework in three key areas:

A. Enhanced cross-border cooperation.

The DFA seeks to consolidate administrative cooperation between consumer authorities through mechanisms for rapid information exchange, operational coordination and joint action, inspired by the DFA model. This approach aims to create a more cohesive regulatory infrastructure, in which national authorities can act collectively against infringements affecting

[22] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004.

multiple Member States, avoiding duplication and ensuring a consistent response. In addition, it contemplates the possibility of establishing lead authorities, similar to those provided for in the GDPR (Art. 56), for cases where a platform is based in one Member State but has an impact throughout the Union.

B. Increased sanctioning powers.

The current consumer protection cooperation (CPC) framework limits sanctioning powers to national authorities, with disparate criteria and wide discretionary margins. The DFA proposes to give enhanced powers to European and national authorities, including the possibility of imposing dissuasive, proportionate and cross-border sanctions, in line with the principle of effectiveness of Union law (Art. 4(3) TEU) and the *Francovich* case law, *C-6/90*[23]. This harmonisation of sanctions is considered essential to prevent 'regulatory forum shopping', whereby large platforms choose to base themselves in countries with more flexible supervisory practices.

C. Technical exchange and digital forensic cooperation.

One of the most significant innovations of the DFA would be the creation of mechanisms for the exchange of technical and forensic information between national authorities, including coordinated access to algorithmic evidence, databases and records of automated decisions. This is essential in an environment where infringements are no longer merely contractual or advertising-related, but technological and systemic, linked to the architecture of digital services. However, the viability of this exchange will depend on the ability of national authorities to handle complex technical data and the existence of common supervisory infrastructures, areas where the EU still has significant shortcomings.

The functioning of digital tools can be extremely complex. A clear example would be Meta's so-called business tools, such as software development kits (SDKs), whose opacity often results in regulatory breaches and harm to consumers[24][25]. This problem stems from a lack of transparency between the developer and the administrator or creator of the technology implemented. Unless algorithmic opacity is tackled through efficient regulation that ensures accountability, automated infringements will continue, and other companies will be discouraged from developing innovative and competitive products.

From a systemic point of view, this reinforcement is essential for the effectiveness of the DFA, as without a uniform and effective enforcement mechanism, the principles of transparency, fairness and comprehensibility risk becoming programmatic mandates with no real operational effect. The experience of the GDPR shows that harmonised *enforcement* and effective institutional cooperation are necessary conditions for ensuring the coherence of the digital single market.

However, the success of the new regime will depend on its organic integration with existing structures, in particular with the institutional framework of the DSA, which already provides

[23] Judgment of 19 November 1991, ECLI:EU:C:1991:428.
[24] *Frasco v. Flo Health*, 349 F.R.D. 557, 568-71 (N.D. Cal. 2025).
[25] Judgement of 4 April 2024, Az. 05 O 2351/23.

for cooperation networks, the appointment of digital service coordinators and a centralised supervision system under the European Commission. It is therefore advisable to link the DFA to these structures through interoperability and mutual recognition mechanisms, avoiding duplication and strengthening administrative efficiency.

In conclusion, the DFA seeks to overcome the structural limitations of the CPC model through an integrated, technological and cross-border enforcement architecture. If it manages to coordinate effectively with the DSA and existing instruments, it could become a true pillar of European digital regulatory governance, capable of ensuring uniform and effective enforcement against digital giants. However, its success will depend on the Union's ability to transform inter-administrative cooperation – currently fragmented and reactive – into a solid, technical and proactive institutional network capable of enforcing the fundamental principle of EU consumer policy: uniform and equal protection for all consumers, regardless of where they are located or the digital provider they interact with.

6. THE INTEGRATION OF COLLECTIVE ACTIONS AS A PROTECTION IN THE DIGITAL ENVIRONMENT

The DFA should expressly recognise the essential role of collective and representative consumer actions as a tool for ensuring the effectiveness of consumer rights in complex digital environments. Given the structural nature of many unfair practices, such as algorithmic opacity, manipulative design patterns or abusive commercial segmentation, individual litigation is often ineffective or disproportionately costly.

Thus, one of Ius Omnibus's first proposals on this issue will be that the DFA contain a specific list of infringements and a provision allowing for collective redress that refers directly to Annex I of Directive 2020/1828[26], relating to the list of rules that fall within the scope of representative actions.

Likewise, for added legal certainty, and to avoid comparative procedural barriers, it would be convenient to add a provision on representation similar to the ones set in article 80 GDPR or article 86 DSA, which give the right to mandate a body their rights in their behalf, thus ensuring more effective and meaningful enforcement.

Particularly, collective actions brought by qualified entities make it possible to correct these asymmetries in an efficient and uniform manner, promoting not only consumer protection but also fair competition and legal certainty for businesses. In this regard, it is important to mention the actions taken in countries such as the Netherlands[27] and Germany[28] regarding

[26] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC.
[27] District Court of The Hague, *Privacy First v. Kingdom of the Netherlands*, February 2020.
[28] TikTok and X collective action for violations of DSA, GDPR and AI Act: https://www.medialaws.eu/tiktok-and-x-faces-class-action-suit-for-violations-of-dsa-gdpr-and-ai-act/

algorithmic transparency and accountability, as they provide valuable precedents and practical insights for addressing digital harms.

The DFA should therefore strengthen the procedural mechanisms for cooperation, access to information and evidentiary presumptions for the benefit of qualified entities, ensuring effective and structurally balanced digital justice.

Rather than facing sector specific barriers, private enforcement and litigation suffer from challenges that must be also tackled to ensure a fair digital environment. To provide a brief list, we shall mention the difficulties or complete inexistence of public funding to advocate for these cases. Among other difficulties, the length of proceedings, the never-ending challenges to legal standing by defendants representing consumers, or the uncertainty in outcomes due to varying criteria in the case law denote a clear trend against enforcement and redress. All the above hinders consumer protection and renders ineffective the efforts to advance the topic of digital fairness.

For such reasons, the DFA should, at least in its Whereas, urge Member States to put in place active procedural measures to prevent lengthy and burdensome proceedings, or any other judicial practices by the parties which may go against the intended objectives of this regulation.

Coordination between the DFA and Directive (EU) 2020/1828 is essential to avoid overlaps and gaps among jurisdictions, ensuring that legitimate associations or bodies have adequate procedural instruments to act against digital infringements. This integration would also make it possible to adapt the burden of proof to the particularities of the digital and algorithmic environment, where relevant information is often under the exclusive control of the platform or service providers.

The coordination of the DFA must be extended to the rest of the EU legal regime to bring about effective enforcement for the digital wrongdoers and redress for the users affected. The effectiveness of digital fairness also relies on certainty regarding jurisdiction (Brussels I Regulation[29]) and applicable law to contractual obligations (Rome I Regulation[30]).

7. PROTECTION IN DIGITAL ENVIRONMENTS: THE CASE OF E-GAMES

The digitization of interactive products, particularly video games, has generated new consumption dynamics marked by a strong information asymmetry between companies and users. The use of opaque algorithms, virtual currencies, random rewards and monetisation mechanisms within the gaming environment itself has created an ecosystem in which consumers, especially minors, find themselves in a position of significant vulnerability.

[29] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[30] REGULATION (EC) No 593/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 June 2008 on the law applicable to contractual obligations.

The DFA aims to update the framework for consumer protection in digital environments. This regulation would complement instruments such as Directive 2005/29/EC, the DSA and Regulation (EU) 2024/1689. However, the preliminary text does not yet address in sufficient depth the particularities of the video game market or the evidentiary difficulties arising from its internal functioning.

Among the most notable risks are the use of virtual currencies or in-game exchange systems that make it difficult to know the real value of the expenditure incurred[31] ; rewards based on chance or uncertainty, such as the well-known *loot boxes,* which introduce elements of randomness and can induce compulsive behaviour; and "pay-to-win" or "pay-to-progress" mechanisms, which generate psychological pressure to spend and may violate the principles of fairness and commercial transparency. Added to this is the absence of effective parental control mechanisms and enhanced protection for minors, despite them being one of the groups most exposed to these commercial gamification strategies.

From a legal perspective, the principle of effectiveness, developed by the case law of the CJEU, requires that the exercise of consumer rights should not be virtually impossible or excessively difficult. This mandate should guide the design of the DFA, incorporating instruments that facilitate proof, reinforce transparency and establish presumptions favourable to the consumer when the trader has a privileged position of information[32] .

Furthermore, from a competition law perspective, the video game industry poses risks to consumers that are at the heart of the DFA's objectives. Specifically, we should mention common restrictions on some video game platforms, such as Most Favoured Nation (MFN) clauses in the sale of download codes. In other words, these are intra-platform restrictions that limit the single market and create discriminatory and unfair situations between consumers in different EU Member States.

Firstly, it would be advisable for the DFA to impose a clear obligation of economic transparency in video games. Any transaction involving real or virtual expenditure should show its price in official currency, alongside the equivalent in the game currency. In addition, the terms of use should include an economic transparency statement detailing the conversion value, spending limits and refund policies. These requirements derive from the principle of pre-contractual information in Directive 2011/83/EU and the doctrine of material transparency established by the CJEU. In this regard, in relation to online platforms accessible to minors, as indicated in the Guidelines on measures to ensure a high level of privacy, security and protection of minors online in accordance with Article 28(4) of the DSA, the DFA should require such platforms to offer minors the opportunity to completely and permanently reset their recommended feeds, ensure that minors can choose an option in their recommendation system that is not based on profiling, regularly test and adapt their recommendation systems to improve the privacy, safety and protection of minors, take into account the specific needs, characteristics, disabilities and additional accessibility needs of minors, and ensure that recommendation systems are not based on the collection of

[31] https://www.osborneclarke.com/insights/digital-fairness-act-unpacked-specific-features-digital-products-particularly-those-common.

[32] King, D. L. & Delfabbro, P. H. (2019). *Video Game Monetization (e.g., 'Loot Boxes'): A Blueprint for Practical Social Responsibility Measures. International Journal of Mental Health and Addiction,* 17(1), 166–179.

behavioural data that captures the activities of minors outside the platform. With regard to random rewards, the rule should require developers to publish in a verifiable manner the probabilities of obtaining each type of result. The lack of such information, or its inaccuracy, should give rise to a presumption of unfair practice, which the operator could only rebut by providing a credible technical explanation. Furthermore, authorities and consumer organisations should be able to audit allocation algorithms under conditions of confidentiality, following the model of access to evidence provided for in Directive (EU) 2024/2853[33] .

Another necessary improvement is the recognition of a right to control monetisation features. Users should be able to disable in-game purchases, random mechanisms or personalised recommendations based on their behaviour. For minors, a version without monetisation elements or, at least, with technical age verification and parental control mechanisms should also be guaranteed. These measures are consistent with Article 25 of the DSA, which prohibits so-called *dark patterns* or manipulative interfaces.

The protection of minors deserves specific treatment. The DFA should expressly prohibit loot boxes paid for by minors without verifiable parental consent and provide for aggravated penalties in the event of non-compliance. Developers, for their part, should implement auditable systems that guarantee the identification of the user's age and the consent of legal guardians.

From a procedural point of view, it is essential to introduce mechanisms that facilitate the burden of proof in both individual and collective litigation.[34] The DFA could establish a presumption of digital unfairness when there are objective indications of irregularities, such as price variations or lack of information on the probabilities of obtaining rewards. In addition, operators should be required to document and retain technical elements related to their monetisation systems and algorithms, allowing consumer associations to access this information under conditions of confidentiality and proportionality.

Overall, the DFA should aspire to be more than just a transparency standard: it should become an instrument that guarantees the real effectiveness of consumer rights in complex digital environments such as video games. Incorporating measures of economic transparency, verifiable disclosure of probabilities, functional control, enhanced protection for minors, evidentiary presumptions and chain liability would balance the relationship between consumers and businesses in the field of digital entertainment, strengthening trust and fairness in the European market.

IV. Conclusion

The DFA represents a decisive step in the evolution of European consumer and digital protection law, aimed at adapting the classic principles of fairness, transparency and protection against unfair terms to the challenges of the algorithmic economy. Compared to

[33] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

[34] Rott, P. (2025). *Digital Fairness and the Burden of Proof. Journal of Consumer Policy,* 48(2). Springer.

a legal framework based on Directive 93/13/EEC, designed for analogue contracts and traditional negotiation contexts, the DFA introduces a comprehensive approach that seeks to redefine contractual justice in digital environments.

Firstly, the proposal addresses the crisis of comprehensibility and transparency in electronic contracts, which are characterised by their opacity, length and legal technicality. In line with the principles of *privacy by design* and *information by design* enshrined in the GDPR, the DFA aims to establish a regulatory framework that guarantees clear, concise and accessible contractual texts that are comprehensible not only from a linguistic point of view, but also in terms of content and functionality. However, the success of this measure will depend on the ability to operationalise the concept of 'comprehensibility' through objective and verifiable methods, such as clarity audits, readability indicators or contractual transparency certifications. A mere formal obligation of clarity runs the risk of becoming symbolic compliance, with no real impact on the consumer's information experience.

Secondly, the DFA introduces an advanced ethical dimension by recognising the inadequacy of the 'average consumer' paradigm in the face of algorithmic personalisation and behavioural manipulation. The creation of a reinforced category of vulnerable consumers – including minors, the elderly and those with low digital literacy – is an explicit recognition of the material asymmetries of power and knowledge in the digital environment. However, its practical application poses sensitive regulatory challenges: identifying these groups without violating privacy, defining specific protection measures, and ensuring compatibility with the principle of technological neutrality. A regulatory balance will be necessary that combines differentiated protection with respect for fundamental rights and regulatory proportionality, preventing good intentions from leading to structural discrimination or unnecessary data processing.

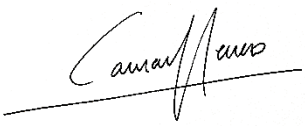
Thirdly, the effectiveness of the DFA will depend on the institutional design of its enforcement system. The current enforcement model, based on the Consumer Protection Cooperation Network, has shown its limitations in the face of global platforms and cross-border infringements. For this reason, the DFA proposes a strengthening of administrative cooperation and sanctioning powers, seeking to ensure uniform application throughout the European Union. This reform must be coordinated with the structures already created by the DSA, avoiding duplication and promoting a coordinated supervisory system capable of sharing technical and forensic information in an agile and secure manner. Only effective procedural and technical harmonisation will make it possible to overcome the current fragmentation and ensure the effectiveness of European consumer law in relation to multinational digital actors.

Overall, the DFA aims to be the cornerstone of a new generation of regulations, consolidating a model of substantive digital protection that goes beyond the formal rhetoric of transparency and information. It is not just a matter of updating legal language, but of redefining the relationship between consumers, technology and the market in terms of justice and shared responsibility.

The challenge will be to put these principles into practice, ensuring that consumers truly understand what they are agreeing to, that vulnerable groups receive effective protection, and that global platforms are accountable to a consistent and uniform sanctions regime. Only through interdisciplinary, coordinated implementation based on technical evidence will the DFA be able to achieve its ultimate goal: to operationalise the principle of digital fairness enshrined in the European Union's legal acquis, ensuring that technological transformation does not erode but rather strengthens the fundamental rights of individuals in the digital environment.

For Ius Omnibus,

Lena Hornkohl, President of Ius Omnibus



Carmen Herrero Suárez, Vice-President of Ius Omnibus

Carmen Estevan de Quesada, Director of Ius Omnibus

IUS OMNIBUS

Avenida 24 de Julho - Second Home Lisboa Mercado da Ribeira, 1200-479 Lisbon

Tel: +351 910 977 799