Ecommerce Europe Submission to Notification no. 2024/0531/ES by the Spanish Government under Directive (EU) 2015/1535 procedure

At Ecommerce Europe, we are committed to fostering a fair and harmonised Single Market. We are therefore compelled to address concerns stemming from the recent notification of the Spanish Government of its Preliminary Draft Organic Law for the protection of minors in digital environments (APLO, for its initials in Spanish).

This document was presented for consultation under the Directive (EU) 2015/1535 (TRIS) procedure and has already been previously submitted to the hearing and public information process by the Ministry of the Presidency, Justice and Relations with the Courts, from 11 to 28 June.

As per our understanding, this measure intends to introduce a series of excessive rules that would undermine the well-functioning of the Digital Single Market. In this document we outline a series of comments we have in relation to the aspects of the APLO that Ecommerce Europe considers to conflict with the European Union regulations, and therefore hinder the proper functioning of the Internal Market.

The recently completed EU legislative cycle has had a very important contribution to the EU's body of law and thus also to the protection of minors. It is important to remark how in recent years, several regulations have been adopted and have entered into force so that ensure a high level of protection of minors against misinformation or access to content intended for adults.

Current EU legislation, including the Audiovisual Media Services Directive (AVMSD) and the Digital Services Act (DSA), require platforms to implement measures to protect minors, including the implementation of age verification systems. However, the proliferation of different national strategies creates an increasingly fragmented market across the EU. **This fragmentation risks hindering the cross-border provision of digital services in the EU, contrary to the objectives of European regulation; and, more importantly, the development of harmonised, user-friendly and truly effective child protection mechanisms.**

In this regard, we believe that **EU Member States need a harmonised framework that applies the same rules for the protection of minors online in all Member States**; a framework that is feasible and technologically viable to implement for the services, applications and content set out in the APLO, without generating a bad user experience. In this context, the strategy presented by Spain insists on a national legislation that, from our point of view, conflicts with several European regulations.

Below, we point out the EU rules and principles with which we consider that the APLO could be in conflict:

1. Free movement of goods and EU single market principles

A central objective of the EU is to achieve a unified Single Market where goods, services and digital activities can move freely across borders. Fragmented national regulations covering digital matters force businesses to adapt to different requirements in each country, contradicting the fundaments of the Digital Single Market and creating obstacles for businesses operating across the EU.

1.1 Operational burden for pan-European businesses

With each EU country implementing unique regulations on digital privacy, protection of minors or data handling, businesses face duplicate compliance costs and operational complexity. Complying with diverse national standards requires re-engineering of products, systems and practices. Pan-European companies must manage overlapping legal standards, which adds technical and administrative burdens. Specifically, potential differing standards on age verification systems may force companies to redesign IT infrastructures and create separate policies, further increasing costs.

1.2 Uneven EU consumer experience, confusion and erosion of trust

EU consumers expect consistent protection and experiences across Member States; however, fragmented regulations lead to varying levels of protection, causing confusion and eroding trust. For example, if one country applies stricter data protection regulations than another, consumers in less regulated areas may lack the same privacy safeguards, creating a fragmented experience that undermines trust in digital services across the EU.

2. Digital Services Act (DSA)

2.1 Contradiction of the APLO with the full harmonisation pursued by the DSA

The DSA is a “maximum harmonisation” instrument, as explicitly stated in Recital 9 of the DSA. In other words, the DSA seeks to create a harmonised Digital Single Market by establishing clear and consistent rules for online intermediation services across the EU. It introduces EU-wide rules to ensure online security, protect fundamental rights and encourage innovation. By establishing this overarching framework, the DSA seeks to prevent Member States from imposing additional national rules that could create inconsistencies and hinder the functioning of the internal market.

Therefore, the DSA applies directly, and Member States should not regulate areas already covered by the DSA unless the rule explicitly states so, which is not the case in the area of the protection of minors in digital environments. Moreover, the DSA itself anticipates the intentions of the Spanish government by warning in Recital 2 that “*Member States are increasingly introducing, or are considering introducing, national laws on the matters covered by this Regulation*” and that “*diverging national laws negatively affect the internal market*”.

2.2. Fragmentation of the digital single market in an area as important as the protection of minors

Specifically, Article 28 of the DSA requires all online platform providers, among other things, to put in place appropriate and proportionate measures to ensure a high level of privacy andsecurity for minors. In addition, very large online platforms and search engines (VLOP and VLOSE) are subject to additional obligations along these lines (Art. 34 and 35). They must conduct annual risk assessments to identify and assess systemic risks arising from the design or operation of their service, or from the use made of their service.

These include actual or foreseeable negative effects on the rights and protection of minors. Where such systemic risks are identified in specific services, online platform providers should implement reasonable, proportionate and effective mitigation measures to address them. This may include age verification tools or parental controls, as well as tools aimed at helping minors report signs of abuse or obtain support resources.

2.3 Overlap with initiatives for the protection of minors in the digital environment

- **Guidelines for the protection of minors in compliance with Article 28 of the DSA**: Article 28(4) of the DSA states that the **European Commission**, in consultation with the European Board for Digital Services, **may issue harmonised guidelines on how online platform providers should meet their obligations on privacy, security, and protection of minors online**. This is expected to happen in the second quarter of 2025. **The European Commission has already set up a taskforce to draft such guidelines and, from 31 July to 30 September, opened the feedback period to contribute to their drafting.**
- **Working group and call for tender for the development of an age verification system**: there is also a working group set up to provide guidance on the more specific issue of age verification, which is composed of the Digital Services Coordinators (DSCs) of the Member States, the European Regulators Group for Audiovisual Media Services (ERGA) and the European Data Protection Board (EDPB). Likewise, from 15 October to 18 November, the Commission launched a call for tenders for the development, consultancy, and support for an age verification system that will allow users to prove their age by presenting an electronic certificate in a way that preserves privacy before accessing age-restricted content. The application will be created in accordance with the EUDI Wallet technical specifications so that it can be integrated into the EU eIDAS2 Regulation from 2026.
- **Better Internet for Kids (BIK+) strategy**: Launched in 2022, this strategy seeks to make online services age-appropriate and ensure that children are protected, empowered and respected online.

For all the above, we advocate **for the support and active participation in the initiatives promoted by the European Commission in the framework of the DSA. This collaborative approach with the European Commission is essential to effectively protect minors online.**

3. European Digital Identity Framework (eIDAS2 Regulation)

As mentioned in the previous section, the European Commission has already started work to develop an age verification system by launching a call for tender for the development, support and consultancy for an age verification system.

According to the call for tender, the European application must be developed in accordance with the technical specifications emerging in the framework of the development of the European digital identity wallet, in compliance with the European Digital Identity Regulation (eIDAS2). In other words, the solution must be able to be integrated into digital identity wallets once they are operational. Given the deadlines, it is foreseeable that this will occur at the end of 2026, so the system proposed by the Spanish government will not be able to meet this requirement.

4. Radio Equipment Directive

We would also like to point out that the obligations for the operating system to activate parental controls by default, and for the manufacturer to provide specific warning information, do not take into account that neither the manufacturer of the device nor the operating system, will have data or knowledge about, among other things, the recommended time of use of products and services. Therefore, this obligation is neither proportional nor consistent with the capabilities of the manufacturer. In addition, the APLO obliges

importers, distributors and marketers to carry out verification of compliance with these requirements and conditions and does not take into account equipment already on the market.

However, **the Radio Equipment Directive (RED) limits the powers of the Member States to legislate in this area with the aim of promoting harmonisation**, establishing in its Articles 3 and 9 that it is up to the EU legislator – and only to it – to define the essential requirements that radio equipment must meet and to determine the rules applicable to its marketing. In this area, the Member States may only regulate the putting into service or use of radio equipment, always in compliance with very specific requirements.

In other words, Member States have no authority to subject the placing on the market of radio equipment to requirements other than those provided for in Article 3 of the RED Directive, such as the mandatory inclusion of parental control functionality.

To avoid the fragmentation of the Digital Single Market, European policy makers should adopt an EU-wide approach to online child safety, including ecosystem-wide initiatives related to parental control. **Rather than discarding existing parental control tools, the aim should be to integrate and enhance them.**

5. GDPR and the Sale of Goods Directive

Similarly, this APLO obliges manufacturers to disclose data protection measures and risks related to privacy and security; however, **there is already a general transparency requirement in the scope of the General Data Protection Regulation (GDPR)**. Similarly, the APLO incorporates the obligation for device operating systems to include parental controls during configuration and to provide warning information specific to the Law on the Protection of Consumers and Users Against Situations of Social and Economic Vulnerability (TRLGDCU) as an objective requirement for device compliance.

However, **the Sale of Goods Directive, already harmonises objective conformity requirements for goods within the EU, so the introduction of this new conformity requirement in the TRLGDCU creates a disproportionate burden for retailers operating within the EU**, in particular those engaged in cross-border trade. Therefore, adding paragraph 7 to Article 115 c of the TRLGDCU seems to conflict with the harmonisation objective of the Sale of Goods Directive, so in order to avoid unintended negative consequences we suggest the deletion of this provision.

6. Electronic Commerce Directive and AVMSD

In parallel, it is necessary to highlight that **the inclusion of age verification obligations in consumer law has the effect of fragmenting the Single Market**. Although "*contractual obligations relating to consumer contracts*" are excluded from the coordinated scope of the **Directive on Electronic Commerce**, this exclusion does not affect the requirements applicable to products and services.

Furthermore, **the Directive on Electronic Commerce establishes in Article 3 the principle of home Member State control**, according to which, on the one hand, "*each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field*", and, on the other hand, specifies that "*Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State*".

The DSA, in line with the Electronic Commerce Directive, upholds the country-of-origin principle as a fundamental pillar of EU law. **This principle ensures that online service providers are primarily regulated by the laws of the EU Member State in which they are established. It prevents Member**

States from imposing additional, potentially burdensome obligations on providers established in other Member States.

Along the same lines, Articles 3 and 4 of the AVMSD provide that "*Member States shall ensure freedom of reception and shall not restrict retransmissions on their territory of audiovisual media services from other Member States for reasons which fall within the fields coordinated by this Directive*", and specify that "*Member States shall remain free to require media service providers under their jurisdiction to comply with more detailed or stricter rules in the fields coordinated by this Directive provided that such rules are in compliance with Union law*".

However, this APLO obliges manufacturers of Internet-enabled devices (e.g., cell phones, tablets, smart TVs and laptops) that offer their devices in Spain, regardless of their establishment, to ensure that the operating system of their devices has a parental control functionality, the characteristics of which will be subject to regulatory development. In this sense, **we understand that imposing a certain model of child protection functionality would infringe the country-of-origin principle, since both the devices and the services, applications and contents can include parental control functionalities certified in other member countries of the European Union**. Similarly, the obligation that the parental control functionality must be activated by default at the time of the initial configuration of the device violates the principle of control in the Member State of origin, since these services and applications may already include parental control functionalities, certified in other EU Member States, and still be blocked at the time of the configuration of the device in Spain.

The same applies to the obligation to provide information on product packaging and in manuals or user guides on risk warnings related to harmful content, data protection, recommended time of use, parental controls, and potential impact on cognitive development, emotional well-being and sleep quality that the APLO includes.

Although the Electronic Commerce Directive provides for exceptions to the country-of-origin principle, these are limited to specific circumstances, namely: (i) specific measures (exceptions only apply to measures taken against a specific online service, not to general regulations); (ii) serious risk (the service in question must pose a demonstrable threat to public order or other vital interests); and (iii) procedural requirements (strict procedural safeguards must be followed, including notification to the provider's home Member State and the European Commission). The DSA, in line with the Electronic Commerce Directive, upholds the country-of-origin principle as a fundamental pillar of EU law. **The APLO does not appear to meet these exception criteria**.

Moreover, the Court of Justice of the EU (CJEU) recently confirmed that a similar national approach was contrary to EU law "*which guarantees the free movement of information society services through the principle of control in the Member State of origin of the service concerned*". Member States should therefore refrain from adopting "*measures of a general and abstract nature that apply without distinction to any provider of a category of information society services*", as this would undermine mutual trust between Member States and conflict with the principle of mutual recognition provided for in the Electronic Commerce Directive.

OTHER COMMENTS

On age verification mechanisms

In recent regulations, age verification systems appear as key elements for the protection of minors in the digital environment. We recognise that age verification systems can be useful solutions for the protection of minors in the digital environment when they are approached from an integral point of view, which also reinforces the responsibility of other actors involved, such as the minors themselves, as well as their families, caregivers and guardians.

In this regard, **we advocate that any age verification mechanism should be approached at EU level, and should always seek to balance risk and proportionality, adopting a risk-based approach.** Specifically, while age verification solutions are useful for the protection of minors online, they also present certain risks and challenges that must be carefully considered and managed, **avoiding creating potentially unfair access barriers and putting the focus at all times on ensuring the efficiency and reliability of these systems and on guaranteeing data protection, the protection of users' privacy and security, the accessibility of digital services, and on respecting the fundamental rights of minors.** We share the approach of experts and organisations in defence of digital rights, who stress the need to seek balanced approaches that minimise risks and maximise the protection of minors in the digital environment.

However, the global nature of both the Internet and the different platforms must also be taken into account, as well as the variety and differences between the services provided by each of them, adjusting the obligations proportionally to the risk that minors face in each of the digital environments. Additionally, it is essential that regulatory standards respect the principle of **technological neutrality,** promoting adaptability and flexibility through self-regulation and co- regulation mechanisms. This would support the development of **future proof systems** that are not outdated in the near future, while encouraging the development of innovative solutions for the protection of minors.

On the obligations of manufacturers of digital devices with Internet connection

The APLO provides that manufacturers of digital devices with Internet connection must include information accessible from their products and on their products, warning of the risks arising from access to content harmful to the health and physical, mental and moral development of minors, as well as information on risks, data protection and recommended time of use. It also establishes that these manufacturers must guarantee that the device includes in its operating system a parental control functionality that allows its users to restrict or control the access of minors to services, applications and contents harmful to minors, and specifies that the activation of this functionality must occur by default at the time of the initial configuration of the device.

It also indicates that manufacturers must accredit to importers, distributors and marketers that the equipment and devices supplied comply with the aforementioned requirements and conditions, and adds that importers, distributors and marketers must carry out verification actions to ensure compliance with these requirements and conditions.

In this regard, we would like to point out the negative impact of these provisions on distributors and manufacturers, who will have to rethink the contractual chain and their agents, but also a significant part of the functionalities of the products offered. We believe that **the implementation of this standard should not lead to a European fragmentation in the event that the Spanish regulations require changes in the historical practices established by each manufacturer.**

In this sense, it is essential to maintain flexibility within the industry, avoiding restrictions and complex local technical adaptations that imply a reform of all production channels to take into account only the specific characteristics of the Spanish market.