MINISTRY OF THE PRESIDENCY, JUSTICE AND RELATIONS WITH THE COURTS

MINISTRY OF YOUTH AND CHILDREN

MINISTRY FOR DIGITAL TRANSFORMATION AND PUBLIC SERVICE

MINISTRY OF SOCIAL RIGHTS, CONSUMER AFFAIRS AND AGENDA 2030.

REF.:
REF.C.M.:

PRELIMINARY DRAFT ORGANIC LAW FOR THE PROTECTION OF MINORS IN DIGITAL ENVIRONMENTS

EXPLANATORY NOTES

I

The development of technology is a constant in our society that generates significant transformations with consequences in various areas of our lives. Particularly relevant is the effect of digitalisation on the personal and social development of minors, which is why it is crucial to have tools and mechanisms to protect and guarantee their rights in digital environments.

The accessibility and globalisation of digital environments allow minors to use these means for exercising fundamental rights, such as the right to information and freedom of expression, and for their political, social and cultural participation at local, national and even international levels.

Alongside the benefits of digitisation processes and universal access to digital environments, it is worth noting the risks and harms that can result from their inappropriate use. The digital environment may include gender stereotyping, discriminatory or violent messages and content, as well as untrue information or information about unhealthy, illegal or harmful behaviour or consumption habits. This information is available to children and adolescents through multiple sources.

Among the risks and harms associated with inappropriate use of digital media and devices, it is worth highlighting the appearance of health issues, both physical, psychological and emotional, difficulties of social interaction or problems in cognitive development. However, in addition to these health risks, there are others related to the use of data and the privacy of minors, the

progressive desensitisation to acts of violence, cyberbullying and the increase in cases of exploitation and abuse of minors.

Access to inappropriate content can produce multiple consequences in childhood and adolescence, as many as varieties of inappropriate content can be considered. Specifically, as can be seen from the Safe Internet for Children initiative (is4k.es) of the National Institute of Cybersecurity (INCIBE), among the potential harm to minors are the following:

- Psychological and emotional harm. Minors have a developing maturity and self-esteem and are therefore more emotionally vulnerable if they are confronted with information that they are not able to handle or to which they do not know how to react, such as, such as pornographic or violent content. These can be too complex and even disturbing.
- Disinformation, manipulation and construction of false beliefs. Untruthful and untrue content can confuse minors, and is especially dangerous when dealing with health and safety issues.
- Establishment of dangerous or socially inappropriate behaviours. Minors can assume certain contents as true and positive, and adopt them in the form of harmful behaviours or values: sexism, male chauvinism, homophobia, racism, etc.
- Damage to physical health. Some content aims to promote eating disorders (anorexia and bulimia), self-harm behaviours or drug consumption. Others may encourage minors to engage in activities potentially dangerous to their health, such as certain videos or viral chains.
- Inclusion in harmful groups and communities. Access to certain content can bring the child closer to extremist, violent or racist groups, as well as sects of an ideological or religious nature, radical political groups, etc. The emotional factor is important when dealing with this information that can be harmful or malicious, since low self-esteem, or that which is still developing, increases the minor's vulnerability.
- Addictions. Addictions. Access to inappropriate content on alcohol, tobacco and other drugs, sex and gambling can promote addiction disorders, as minors may not have sufficient critical capacity to manage the risks associated with these types of activities.
- Economic expenses. Frauds or deception attempts aimed at defrauding users to obtain their money or data can lead to direct economic losses, as is the case for example with Premium SMS subscriptions. In addition, minors are more vulnerable when it comes to interpreting and managing the excessive advertising to which they are exposed on the Internet since it can generate in them the need to consume impulsively, as happens with purchases in games and applications. Likewise, the content of the ads is not always, in itself, suitable for them.

In this vein, it is necessary to advance in the protection of children, adolescents and youth to generate an increasingly safe digital environment, aimed at guaranteeing their integral development, avoiding the risks and dangers that have been pointed out both from scientific and educational fields and from the entities and associations for the protection of children and youth. Likewise, digital training should be promoted in order to teach children and adolescents to be conscious and safe users of technology, as well as psychological aspects taking into account the emotional and cognitive impact of online experiences.

Spain is committed to the rights of children and adolescents, as evidenced by the ratification of various international human rights agreements, including among others the Convention on the Rights of the Child, as well as policies to promote these rights and combat violence against children. Taking into account that digital environments are today one of the different areas in which life in society develops, this standard is necessary to regulate and guarantee the enjoyment of children's rights in these environments. This provision therefore derives from Article 20(4) of the Spanish Constitution, which recognises special protection for young people and children, and from Article 39, which lays down the right to comprehensive protection for children. Articles 33, 45 and 46 of Organic Law 8/2021 of 4 June on the comprehensive protection of children and adolescents from violence, among others, also constitute precedents for the legislation. Given the reality of the opportunities and risks posed by digital environments, it is up to the State to put in place measures to ensure the enjoyment and promotion of the rights of children and adolescents in this field.

Measures and proposals for the regulation of digital environments with regard to minors have also been promoted at European level. The Strategy for the Rights of the Child 2021-2024 drew attention to this issue, with the digital and information society being one of the six thematic areas this comprises. In addition to pointing out its enormous potential in the field of education or for reducing certain social gaps, it points to the need to take measures to address the risks that the digital world can bring in areas such as cyberbullying or hate speech, as well as the need to introduce regulation to avoid health problems that can arise from excessive exposure to screens. The European Strategy for a Better Internet for Children pointed in the same direction that different countries around us have already regulated or are in regulatory processes.

This standard also responds to the different indicators of both supranational institutions and different relevant actors of civil society that place some of the problems derived from the exposure of children and adolescents to digital environments, in a deregulated way, as a public health issue. This regulation therefore guarantees the right of children to grow up without their development being conditioned by exposure to screens, as well as to be able to make use of digital environments in a positive way, either in the field of education or as a space for social interaction or access to culture and leisure.

In addition, and in view of the need to make progress in the protection of children and adolescents in the digital spheres, the Government established, by agreement of the Council of Ministers of 30 January 2024, a Committee of Experts for the Development of a Safe Digital Environment for Youth and Children. This Committee, consisting of representatives of civil society, representatives of different institutions, academics specialised in different elements linked to this problem, and representatives of the organisations of child and adolescent participation themselves, as well as entities responsible for the promotion of their rights, has been working on digital environments with a multidisciplinary and intersectional look in order to make a report that analyses good practices and develop recommendations, measures and actions for a road map with the aim of generating a safe digital environment, which contributes to the better protection of the integral development of children and adolescents.

The standard is also inspired by the work that has been carried out in different spaces to address the elements that find their reflection in the norm that, given the complexity of the problem,

integrates them from different perspectives. This thus brings together proposals concerning the digital sector, service providers in this field, and also the development of policies in the fields of education, health, or consumer protection policies.

In this sense, the generation of safe spaces in the digital field for children and adolescents cannot be done with their backs to that part of the population. The standard therefore gives an active role to children and adolescents, recognised as subjects of rights that, through tools that are generated such as the National Strategy on the Protection of Children in the Digital Environment, can participate in the design, monitoring and evaluation of public policies derived from the implementation of this Law that concern them directly. In short, what is to be delimited through the law is the right to protection against digital content that may be harmful to their development and their right to be able to make decisions about them, receiving information appropriate to their age. These rights of children and adolescents are developed through the measures and policies described in the articles of the law, as well as the different obligations deriving from them for the administration and the private sector, which plays a fundamental role in this field. The regulation thus generates the necessary framework for the development of the commitments made by Spain in terms of the rights of minors in the face of the growing role played by digital environments as one more plane in which society develops.

II

The preliminary title, 'General provisions', constitutes the basic frame of reference to guarantee respect and equal enjoyment of all children and adolescents in digital environments, encouraging the active participation of this group and overcoming the barriers of discrimination.

The main objective of the law is to provide safe digital environments for children and adolescents, with full protection of their rights and freedoms, while encouraging the proper and respectful use of new technologies.

In accordance with the above, Article 2 recognises the rights of minors in this type of environment, including the rights to be effectively protected against digital content that may harm their development, to receive sufficient and necessary information in an age-appropriate form and language on the use of technologies and the risks associated with it, as well as equitable and effective access to devices, connection and training for the use of digital tools.

This completes the framework previously defined by Organic Law 1/1996 of 15 January on the Legal Protection of Minors, partially amending the Civil Code and the Law on Civil Procedure; Organic Law 8/2021 of 4 June on the comprehensive protection of children and adolescents from violence, Title III, with Chapter VIII of which being dedicated to new technologies, promoting public-private collaboration in order to ensure the safe and responsible use of the internet and information and communication technologies among minors; and Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights, which provides for the need to grant real protection to minors on the internet, to which end it obliges parents, guardians, carers or legal representatives to ensure that minors make balanced and responsible

use of digital devices and information society services in order to guarantee the proper development of their personality and preserve their dignity and fundamental rights (Article 84); obliges educational establishments and any natural or legal persons carrying out activities involving minors to ensure the protection of the best interests of the child and his or her fundamental rights, and in particular the right to the protection of his or her personal data on the internet (Article 92); It provides for the adoption of an Action Plan to promote the training, dissemination and awareness-raising actions necessary to ensure that minors make balanced and responsible use of digital devices and equivalent social networks and information society services on the Internet, in order to ensure their proper development of personality and to preserve their dignity and fundamental rights (Article 97(2)).

Along the same lines, Article 3 sets out the aims of the standard to ensure respect for and compliance with the rights of children and adolescents in the digital environment, especially the rights to privacy, honour and self-image, as well as the best interests of the child in the development of digital products and services, and to promote a balanced and responsible use of digital environments, support the development of children's digital skills in the digital environment to make it a safe place, among others.

The measures included in the law are deployed from a broad and multidisciplinary perspective, reaching a comprehensive protection of minors in the use of devices and digital media with a preventive, care and inclusion perspective, in order to offer through the appropriate channels tools to anticipate the development of more serious issues, and promote environments without discrimination.

III

The digital environment offers many advantages and benefits to society as a whole, but its use must be particularly appropriate when the main recipients of new digital technologies are minors, who increasingly face greater risks from harmful consumption.

That is why this Law contemplates several measures in the field of protection of minors as consumers and users, which are included in Title I and also in the fourth final provision, which expressly modifies the consolidated text of the General Law for the Protection of Consumers and Users and other complementary laws, adopted by Royal Legislative Decree 1/2007 of 16 November.

With regard to the measures set out in Title I, Article 4 establishes two new obligations addressed to manufacturers of digital terminal equipment with an internet connection through which minors can access content harmful to their development, which are in line with the provisions of Article 46(3) and (4) of Organic Law 8/2021 of 4 June: an obligation to inform their products of the possible risks arising from misuse, inter alia, and an obligation for the digital terminal equipment they manufacture to include in their operating system a parental control functionality that allows their users to restrict or control the access of those persons to services, applications and content

harmful to minors, the activation of which must occur by default at the time of the initial configuration of the terminal equipment.

As a more specific situation, consumption with a harmful potential includes random reward mechanisms (‘*loot boxes*’), which are part of some video games and which, without proper access control in their activation, may pose a risk to vulnerable people, especially the younger ones to whom they are addressed and who are the main consumers of this type of products and services, as evidenced by the study ‘Loot boxes in online games and their effect on consumers, in particular young consumers’, commissioned by the Committee on the Internal Market and Consumer Protection of the European Parliament, which draws attention to the different risks associated with the mechanisms used in loot boxes depending on the stage of development of children and adolescents.

Random reward mechanisms are virtual objects or processes of any kind whose activation offers the player the opportunity to obtain, on a random basis, virtual rewards or prizes that can be used in those digital environments.

As the scientific literature has revealed, the evident functional identity of some of the modalities under which these random reward mechanisms are presented with traditional gambling also brings with it the negative consequences associated with the latter, such as the emergence of thoughtless, compulsive and, ultimately, pathological consumption behaviours. All of this based on the mechanics of psychological activation that can be triggered by participating in this activity, which is the cause of serious economic, patrimonial and affective repercussions, both in the people who suffer them and in their personal, social and family environment.

In the case of minors, contact with these random reward mechanisms is likely to constitute their first encounter with a product or functionality in the operational mechanics of which chance plays a predominant role, and which bears the aforementioned similarity, both from the structural point of view and from the marketing techniques used for its marketing, with certain modalities specific to regulated gambling.

For these reasons, Article 5 provides for a general prohibition of access to random reward mechanisms or their activation by minors, although by regulation cases may be established in which exceptions are determined in which the prohibition is relaxed, provided that the protection of children is guaranteed.

It is clarified that the aforementioned prohibition and the consequent obligation to establish an age-verification system prior to access to this type of products and functionalities does not operate in a general way, but applies only to random reward mechanisms that have a set of characters that make them more similar to certain gambling products. Consequently, not all processes, functionalities or products associated with interactive leisure software products that integrate chance as an essential element of their structural configuration are subject to this regulation. In addition to the payment of a price for the activation and the presence of the element of chance, the law includes under its scope only those random mechanisms that grant rewards consisting of a virtual object that can be exchanged for money or other virtual objects.

In line with the measures referred to in Title I, the fourth final provision amends the recast text of the General Law for the Protection of Consumers and Users and other complementary laws,

adopted by Royal Legislative Decree 1/2007 of 16 November, in order to incorporate the protection of minors, as vulnerable consumers, in relation to digital goods or services. In addition, there is an obligation on the business side to ensure the age of majority of the consumer and user prior to contracting goods or services of their own or others or, internally or externally, intended for adults, either because of their sexual, violent content or because they pose a risk to physical health or the development of personality; The breach by the trader of this age verification and check obligation is categorised as a minor infringement in terms of consumer and user protection.

IV

Title II, consisting of Articles 6 and 7, incorporates measures aimed at the field of education.

The current educational legislation promotes the use of new technologies in teaching, contributes to the improvement of students' digital skills, and assumes the need for the digitalisation of the educational field to be accompanied by economic, social and gender inclusiveness in access to technologies, and a safe and respectful use of digital media with constitutional values and rights.

The growing concern to avoid the risks of inappropriate use of information and communication technologies and the social debate surrounding these situations has attracted the attention of educational administrations. Thus, in 2024, the Ministry of Education, Vocational Training and Sports and the Autonomous Communities shared views on ways to address these issues, and the State School Council approved a proposal to regulate the use of mobile phones in schools during school hours. It is a series of recommendations and conclusions such as the zero use of mobile phones in both early childhood education and primary education, and that these devices remain deactivated throughout school hours in secondary education, and can be used in the event that the teacher considers it necessary for a specific educational activity. In any case, exceptions are provided for health, safety or special-needs reasons.

In its handling of the problems identified, Article 6 of this Law responds to the need to improve training in this area for both students and teaching staff.

On the one hand, it provides for the promotion of actions to improve the digital skills of students, in order to ensure their full integration into the digital society and the learning of a safe, sustainable, critical and responsible use of digital technologies for learning, work and participation in society, as well as interaction with these. These provisions are in line with the pedagogical principles developed by Organic Law 2/2006, of 3 May, on Education, one of which is precisely the transversal development of digital competence, and are also linked to Article 5 of Organic Law 1/1996, of 15 January, in relation to the right to information, and Article 33 of Organic Law 8/2021, of 4 June, on training in the field of rights, security and digital responsibility.

On the other hand, the fundamental role of teachers in the process of acquisition of digital skills by students and in the detection of risks is recognised, and therefore it is provided that the planning of the continuous training of teachers incorporates training activities that provide teachers with strategies for the handling, among other aspects, of security and elements related to digital

citizenship, privacy and intellectual property, taking as a reference the areas and competences established in the Framework of Reference of the Digital Teaching Competence and the existing regulation in terms of comprehensive protection of children and adolescents against violence, protection of personal data and guarantee of digital rights.

Finally, in a more specific way regarding the problem mentioned above, Article 7 establishes that educational centres, in accordance with the provisions approved for this purpose by the educational administrations, regulate as part of their rules of operation and coexistence the use of mobile and digital devices in classrooms, in extracurricular activities and in places and rest times that take place under their supervision.

V

Title III provides for measures in the field of protection of victims of gender-based violence and sexual violence.

Thus, Article 8 establishes that victims of gender-based violence or sexual violence facilitated by digital environments will have the status of victims for the purposes of Organic Law 1/2004, of 28 December, on Comprehensive Protection Measures against Gender Violence and Organic Law 10/2022, of 6 September, on comprehensive guarantee of sexual freedom, respectively.

These equivalences are consistent with Article 14 of the Council of Europe Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse, done in Lanzarote on 25 October 2007, and Article 26 of the Council of Europe Convention on preventing and combating violence against women and domestic violence, done in Istanbul on 11 May 2011.

Article 9 ensures that minors have the right to access information and guidance services and, where appropriate, immediate psychosocial care and legal advice, by telephone and online, 24 hours a day, every day of the year.

Similarly, the right to access reception services and psychological and social assistance for victims of gender-based violence and sexual violence and 24-hour crisis centres is recognised.

In addition, it is deemed essential to consider these services as essential, since they depend on the safety, health and well-being of the affected population that is especially vulnerable.

VI

Title IV deals with health measures to be taken by public administrations.

The impact on the health of children and adolescents due to the inappropriate use of digital technologies and environments is a growing concern for families, educators and health professionals. Although there are numerous studies, the results of these are sometimes contradictory or inconclusive. However, there is evidence that excessive screen time and

exposure to inappropriate content can affect mental health and increase the risk of anxiety, depression, addiction, self-esteem issues, sleep disorders, problems with language development and social skills, as well as the ability to concentrate and solve problems.

Evidence has also been found that adolescents with high exposure to digital media and environments might be more likely to develop symptoms of attention deficit hyperactivity disorder. In addition, children may be exposed to hate speech, violence and content that incites self-harm or suicide, or that has a negative impact on their emotional and psychological well-being.

On the other hand, excessive time in front of screens contributes to a sedentary lifestyle and therefore to suffering from musculoskeletal disorders, childhood obesity and the problems derived from this, such as cardiovascular and endocrine diseases. In addition, exposure to screens can affect the quality and habits of sleep as well as visual health and lead to blurred vision problems, dry eyes and headaches, as well as sleep disorders.

It becomes necessary, therefore, to establish health measures for the prevention of health problems arising from the misuse of digital technologies and environments and promote healthy habits of use.

To this end, Article 10 promotes that, based on the principle of health in all policies, the health dimension be incorporated into the studies promoted by public administrations on the use of these technologies and digital environments by minors, with the aim of increasing knowledge about the effects on health and generating scientific evidence. In addition, it incorporates individual and community actions in the programmes of prevention and promotion of child and adolescent health that are developed from primary care, for the early detection of specific problems related to digital technologies and environments, as well as the establishment of coordinated programmes with other public administrations, for the comprehensive approach, treatment and rehabilitation, with a biopsychosocial perspective.

On the other hand, Article 11 promotes specialised health care for minors with addictive behaviours without substance.

VII

The measures in the public sector, regulated in Title V, are based on the obligation of the public authorities to promote the conditions of freedom and equality of persons, both individually and in the groups in which they are integrated, so that they are real and effective, removing the obstacles that hinder their fullness and facilitating citizen participation in the social, political, cultural and economic sphere, as set out in Article 9(2) of the Spanish Constitution. In addition, pursuant to Article 11 of the Organic Law 1/1996 of 15 January, public administrations should take into account the needs of minors when exercising their powers, in particular in relation to new technologies.

Through the participation, information and awareness-raising measures provided for in Article 12, in line with the provisions of Organic Law 8/2021 of 4 June, emphasis is placed on the need to

incorporate proactive and effective actions in relation to information and training on safe digital environments, aimed at minors and their families, ensuring the effective exercise of the right to participate in plans, programmes and policies that affect children and young people.

Article 13 provides for the promotion of public-private collaboration and co-regulation, so that providers of internet access service from a fixed location approve a code of conduct that establishes the mechanisms and parameters of secure configuration that they undertake to apply in the provision of their services in places of public access where public services are provided, to avoid minors accessing inappropriate content.

Article 14 ensures professional specialisation at all levels of the administration for all staff working in direct contact with minors.

To that end, the provision mandates the Government, in collaboration with the Autonomous Communities, to develop a framework programme for the training and retraining of these professional sectors that covers, in addition to the specific aspects related to each sector, gender stereotypes, trauma and its effects and responsibility in reducing secondary victimisation.

Article 15 sets out the Government's obligation, in collaboration with the Autonomous Communities, the cities of Ceuta and Melilla and local authorities, to draw up a national strategy on the protection of children and adolescents in the digital environment, in which the Children's Observatory, third-sector bodies, civil society and, in particular, children and adolescents will participate. This Strategy, to be defined in line with the State Strategy for the Rights of Children and Adolescents, will pursue digital and media literacy, the dissemination of information to families, and persons who are habitually in contact with minors, the safe use of devices, research and the creation of spaces for interaction and collaboration on digital culture.

VIII

The protection of minors in digital environments may require as a last resort the disruption of an information society service offering unlimited access to content that seriously harms the physical, mental and moral development of minors. In general, Article 8(1) of Law 34/2002 of 11 July on information society services and electronic commerce allows the bodies competent for its protection to take the necessary measures to interrupt the provision of an information society service or to withdraw the data it offers.

Since these restrictive measures may affect fundamental rights such as freedom of expression or the right to information, which enjoy constitutional protection, an order for the interruption of a service or the removal of content must have the corresponding judicial authorisation.

However, the judgement of the Supreme Court 1231/2022 of 3 October, warned the legislature of the existence of a loophole in this regard in our procedural legislation, where a procedure is only

provided for requesting judicial authorisation of the measure when it comes to the safeguarding of intellectual property rights and so requested by the Second Section of the Commission on Intellectual Property, with the omission of the other cases provided for in Article 8(1) of Law 34/2002 of 11 July, including the protection of youth and children, which empower the competent authorities by reason of the matter to adopt, with judicial authorisation, this type of measure. The same gap is observed for the acts adopted for the limitation of access to an intermediary service provided for in Article 51(3)(b) of 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 (Digital Services Act).

In order to fill this legal gap, the first and third final provisions of this Law respectively amend Organic Law 6/1985 of 1 July, the Judiciary and the Law 29/1998 of 13 July, on Contentious-Administrative Jurisdiction.

Specifically, Article 90 of Organic Law 6/1985, of 1 July 1985, and Article 9(2) of Law 29/1998, of 13 July, are amended in order to confer on the Central Administrative Courts the power to authorise the execution of acts adopted by the administrative bodies competent in the matter to interrupt the provision of information society services or to remove content that violates any of the legal assets listed in Article 8 of Law 34/2002, of 11 July, not only intellectual property, as well as for the execution of those adopted for the interruption of access to an intermediary by a digital services coordinator based on Article 51(3)(b) of the Digital Services Regulation, or pursuant to Article 93(4) of Law 13/2022, of 7 July, General Audiovisual Communication.

Article 122 bis of Law 29/1998 of 13 July is also amended so that the judicial authorisation procedure for the execution of these measures is generalised for all protected legal assets, not only to safeguard intellectual property.

With regard to the protection of minors in digital environments, the authorisation of the Central Administrative Courts to authorise these measures will allow all the competent authorities in the matter to request judicial authorization for the interruption of services or removal of content that threatens the protection of youth and children. Among other scenarios, this would allow the National Commission on Markets and Competition to request authorisation of a cease-and-desist order from a video-sharing platform or on-demand audiovisual media service with adult content that does not include age verification systems that limit their access to minors.

IX

The reduction of the risk associated with the use of digital technologies by minors also necessitates the reform of the Criminal Code, which is carried out in the second final provision.

Certain technological crimes aimed at the protection of minors have been covered by the latest reforms of the Criminal Code, mainly that produced by the sixth final provision of the Organic Law 8/2021 of 4 June on comprehensive protection of children and adolescents from violence, where for the first time there is talk of digital violence. This reform has punished behaviours of

distribution or public dissemination through the Internet, by telephone or any other information technology or the communication of content specifically intended to promote, encourage or incite suicide, self-harm or behaviours related to eating disorders or to aggressions sexual to minors. Also included in the different precepts of the Criminal Code is the blocking and removal of *websites*, internet portals or applications containing or disseminating child pornography, encouraging hatred of groups or extolling or justifying terrorism (Articles 189(8), 510(6) and 578(4) of the Criminal Code); and, in the same way, the Organic Law 13/2015 of 5 October amending the Code of Criminal Procedure to strengthen procedural safeguards and regulate technological research measures, incorporated Articles 588 bis to et seq. on the investigation of criminal offences committed through computer tools or any other information or communication technology or communication services.

However, there are other situations directly related to minors safely accessing the Internet, which involve not only with the modification or creation of figures specifically aimed at the guardianship of minors, but also with the problems arising from a lack of adaptation of the current standard to new technological advances.

It is therefore necessary to introduce certain changes in the Criminal Code that advance in adapting it to the new forms of crime and that, without forgetting the limiting principles of *ius puniendi* of the State, allow exercising effective protection against the new technological crimes.

In line with this objective, it has been considered appropriate to incorporate four types of modifications, which are articulated in the second final provision.

First, it incorporates the penalty of not accessing from virtual environments, for better compliance with general and special prevention in the field of technological crimes. Specifically, Articles 33, 39, 40, 45, 48, 56, 70 and 83 of the Criminal Code are amended to incorporate the penalty of prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space, when the crime is committed within this.

In this way, the content of the penalty is linked to the nature of the crime, and greater protection of victims is established. avoiding the repetition of punishable conduct.

The need is also verified if the judgment of the Supreme Court 547/2022 of 2 June is complied with, which accepts as possible the imposition of the penalty of prohibition on the accused from going to the place of the crime, this being a virtual site. The High Court confirms in this resolution what was already announced doctrinally: in technological crimes, a distinction must be made between the means of commission and the place of commission. In this regard, it states that '*(T)he more recent experience teaches that social networks are not only the instrument for the commission of some crimes of a very different nature. They can also be the scenario in which the crime is committed, either throughout its development or in the execution of only some of the elements of the type'.*

Faced with the great increase in virtual crime, social networks are a place where crimes are frequently committed or where the execution of acts initiated or partially executed is prolonged and the introduction of the penalty of *prohibition to access or communicate through social networks, forums, communication platforms* or any other place in the virtual space gives an answer effective the growing cybercrime, by preventing the repetition of punishable behaviour in

virtual spaces and improving the protection of victims by preventing their secondary victimisation. Its explicit incorporation into the Criminal Code means that its application is better adapted to the principles of legality and criminality, and its provision is also made in terms appropriate to the principle of proportionality, since its extension must be specified on a case-by-case basis by means of a duly motivated judicial decision that must allow the sentenced person access to other networks or virtual spaces not directly related to the crime committed.

Second, it specifically addresses the criminal treatment of so-called *deepfaking*, this is technologically manipulated and extremely realistic images or voices. To this end, a new Article 173 bis is incorporated, which penalises those who, without the authorisation of the affected person and with the aim of impairing their moral integrity, disseminate, exhibit or cede their body image or voice audio generated, modified or recreated through automated systems, software, algorithms, artificial intelligence or any other technology, in such a way that it seems real, simulating situations of sexual or seriously vexatious content.

In addition to the fact that deepfaking is generally disseminated in cyberspace, with the potential for permanence that this implies, as has been noted with respect to technological content crimes, there is an increase in harmfulness in relation to other forms of attack due to the enormous difficulty of distinguishing between false and real content due to the accuracy of new technologies and the greater degree of veracity we maintain with respect to audiovisual materials on written materials.

Technically, the sanction is chosen for the dissemination of deepfakes of sexual content (known as *pornographic deepfakes*) or especially vexatious in the case of crimes against moral integrity because, under the principle of consumption, the cases of damage to moral integrity and also attacks against honour would be covered, since it is necessary to take into account not only the affectation to self-esteem and self-esteem, but also the objectification and instrumentalisation that occurs on the passive subject, usually women and girls, children and adolescents who are treated as objects of consumption. We must also remember that the motivation to carry out these actions is not always identified with the *animus iniuriandi*, as the fact may be due to other reasons such as profit motive, if such images are used in pornographic content pages or applications.

Third, given that the specific objective of the law is to protect the interests of children and adolescents, and that there is great concern regarding children's access to pornographic content that may affect their development in the sexual affective sphere, the amendment is envisaged. of Article 186 of the Criminal Code, with the aim of improving the protection of the legal good sexual freedom of minors.

As currently drafted, Article 186 of the Criminal Code punishes those who ‘by direct means’ sell, display or disseminate pornographic material to minors and persons with disabilities in need of special protection. Such wording does not sufficiently protect the legal good of sexual intangibility of these groups against the indiscriminate availability of this type of material in media in which, knowingly, it will be accessible to them. Consequently, the reform of this provision is addressed, which has a special impact when it comes to minors. With the new wording that is incorporated, it is possible to punish cases in which pornographic material is made available to an indiscriminate group of users, among which there is a clear representation that there will be minors. To this end, a specific reinforced intent is also considered. It is not enough, for punishing the conduct, that it be

committed deliberately as to the objective data of the transmission or dissemination of the material, but there must be a clear awareness that among the receiving public there are minors or people in need of special protection, and that the consumption by these subjects of this type of material implies an affectation to their process of sexual maturation.

Fourth, in line with the target indicated, and taking into account the impact of the assumptions of masking one's identity in this area, different aggravated types are also introduced in Articles 181, 182, 183, 185, 186, 188 and 189 dealing with the use of false identities through technology, which facilitate the commission of crimes against minors.

X

On the other hand, Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights is also modified through the fifth final provision to raise the age from which minors can give consent for the processing of their personal data to 16 years.

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 (General Data Protection Regulation) provides that where consent is the legal basis for the processing of data in information society services, such consent may be given by a minor if he or she is at least 16 years of age; the consent of the holder of parental authority or guardianship over the child for younger ages is necessary. It also allows countries to reduce the previous limit from 16 years to a minimum of 13 years.

Using this authorisation, Organic Law 3/2018, of 5 December, established the threshold of 14 years for the consent of minors. However, the evolution not only of digital technology, but also of its use by minors has been so exponential that its early use may be inappropriate; given the maturity required for the use of certain digital services, platforms, systems and content.

Therefore, it is considered necessary to raise the age of consent of the child in terms of data protection, harmonising the threshold with that established by most countries of the European Union, as well as with the one required in the national legal system for minors in other activities or behaviours.

XI

Finally, this Organic Law, through its sixth final provision, it incorporates nine amendments to Law 13/2022 of 7 July.

First, Article 3 on the scope is amended to, on the one hand, oblige to comply with the provisions of Article 99(1), (2), (3) and (4) and Section 1a of Chapter IV of Title VI of Law 13/2022 of 7 July, the audiovisual media service provider that, being established in a country that is not a member of the European Union or the European Economic Area, specifically directs its services to the Spanish market. On the other hand, it is obliged to comply with the provisions of Articles 88, 89, 90 and 91 of Law 13/2022, of 7 July, to the provider of the video-sharing platform service that, being established in a country that is not a member of the European Union or the European Economic Area, directs its services specifically to the Spanish market, provided that this does not contravene the provisions of applicable international treaties or conventions.

Second, in order to improve the effectiveness of the reporting channels established by the audiovisual supervisory authority, Article 42(b) is amended so that audiovisual media service providers and video-sharing platform service providers include on their corporate websites an easily recognisable and accessible link to the website of that authority. Likewise, this obligation is extended in a similar way to users of particular relevance who use video-sharing platform services.

Third, Article 89 on measures for the protection of users and minors from certain audiovisual content is amended in order to strengthen the measures currently in place to prevent the exposure of minors to content inappropriate to their age. Specifically, it provides that age verification systems must ensure security, privacy and data protection, in particular as regards data minimisation and purpose limitation. In relation to the above, the future European Digital Identity Wallet (EUDI Wallet), which all Member States are required to provide by November 2026, pursuant to Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European Digital Identity Framework, is a benchmark for the highest standards of security, privacy and data protection, which will allow European citizens to access public and private services, with full control over the data they share with third parties. In particular, one of the possible use cases of the EUDI Wallet is age verification. In this sense, the age verification systems established in compliance with the regulations should be inspired by the aforementioned security, privacy and data protection standards of the future EUDI Wallet.

Likewise, the provider is required to establish parental control systems controlled by the end user with respect to content that might harm the physical, mental or moral development of minors.

Article 93(4) is also amended, which provides that failure to comply with the obligations laid down in Article 89(1)(e) will constitute the offence referred to in Article 157(8), without prejudice to any criminal liability that may arise from such action. In this regard, a provision is included to expressly provide that the National Commission on Markets and Competition may adopt the measures provided for in Articles 8 and 11 of Law 34/2002 of 11 July, in accordance with the provisions of those articles.

In addition, Article 94(1) concerning the obligations of users of particular relevance using video-sharing platform services is amended. These services, which, in many fields, are grouped under the concept of ‘vloggers’, ‘influencers’ or ‘opinion leaders’, are relevant in the audiovisual market from the point of view of advertising and consumer investment, especially among the younger audience.

Article 94 currently imposes a number of obligations on users of particular relevance aimed at reducing the exposure of users of video-sharing platform services to harmful or harmful content, and in particular with regard to child protection obligations, they were assimilated to on-demand audiovisual media services.

Since the adoption of Law 13/2022 of 7 July, new video-sharing platform services have appeared that can no longer be deemed comparable to on-demand services, since users of particular relevance offer live audiovisual content, much more similar to linear audiovisual media services. Therefore, in order to ensure adequate protection of minors from exposure to harmful or harmful content, it is considered appropriate to amend the regime established in Article 94(1) and extend to users of particular relevance compliance with the obligations for the protection of minors from harmful content laid down in Article 99(2) and (3) depending on whether the type of service they offer can be considered linear or on-demand.

Likewise, the reform aims to increase legal certainty since the changes introduced seek to clarify, among other aspects, that users of special relevance must qualify the content they generate and upload to video-sharing platform services.

Sixth, Article 99(3) and (4) concerning content harmful to the physical, mental or moral development of minors are amended by obliging conditional access linear television audiovisual media services and on-demand television audiovisual media services to establish age verification systems for users.

In addition, Article 155 is amended so that the National Commission on Markets and Competition (CNMC) supervises and controls compliance with the provisions of Law 13/2022 of 7 July, except as regards qualifying titles, and exercises the power to impose penalties, in accordance with the provisions of Law 3/2013 of 4 June, in respect of television audiovisual media service providers and video-sharing platform service providers established in a country that is not a member of the European Union or the European Economic Area that specifically direct their services to the Spanish market.

Eighth, Article 160(1)(c) is amended in order to strengthen the sanctioning powers of the CNMC, allowing that body to impose as ancillary sanctions, on the one hand, the cessation of the provision of the service and the loss of the status of provider acquired through prior communication, for a maximum period of one year, when the very serious infringement provided for in paragraphs 13 and 14 of Article 157 has been committed, and on the other hand, the cessation of the provision of the service by the provider of the video-sharing platform service, for a maximum period of one year, when the latter has committed the very serious infringement provided for in Article 157(8), consisting in the breach of its obligation to establish and operate age verification systems for users with respect to content that may harm the physical, mental or moral development of minors who, in any case, prevent them from accessing the most harmful audiovisual content, such as violence free of charge or pornography.

Finally, Article 164(1) is amended so that, once the penalty procedure has been initiated for one of the very serious infringements referred to in Article 157(8) and (14), measures may be adopted that include the interruption of the offending service and the removal of data.

XII

In drafting this Organic Law, the principles of good regulation referred to in Article 129 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations have been observed; that is, the principles of necessity, effectiveness, proportionality, legal certainty, transparency and efficiency.

With regard to the principles of necessity and effectiveness, the foregoing points to the need for each of the measures adopted, which are considered to contribute effectively to improving the protection of minors in the digital environment.

Although the measures for the protection of minors established by the standard have for the most part a positive content, strengthening their rights in the digital field, it also entails the imposition of certain new obligations, particularly for companies providing digital devices, services and content. In accordance with the principle of proportionality, care has been taken to ensure that the scope and content of these obligations are essential to ensure the protection of minors. This same principle of proportionality inspires the configuration of the reforms of the Criminal Code, as explained above.

The law also meets the requirements of legal certainty because, on the one hand, it seeks to clearly define the measures it incorporates, and on the other, some of them are specifically aimed at improving the precision, clarity and completeness of our current legislation.

In accordance with the principle of transparency, the procedure for drawing up the standard has made it possible for potential recipients to participate. Likewise, the standard defines the objectives of the measures that it incorporates and both its expository part and the report of the normative impact analysis contain an explanation of the reasons that justify them. From this same perspective it is finally noteworthy that some of the measures it contains are specifically aimed at reinforcing transparency in this field, and therefore it is imposed on public administrations the duty to promote the consultation and participation of minors in the adoption of measures that can guarantee their rights in the digital field, as well as the use of clear language, so that public administrations and entities of the private sector use a language accessible to minors in the communications addressed to them and in the information to which they have access.

In application of the principle of efficiency, the law does not incorporate new administrative burdens, and seeks to rationalise public spending to the extent that its compliance will be met with the resources that are indispensable and promotes coordination and collaboration between public administrations in the adoption and implementation of measures involving several of them, which is understood to result in a more effective and efficient application of public resources.

In the processing of this Organic Law, the procedure for the information of technical regulatory standards and regulations relating to information society services, provided for in Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and rules on information society services, as well as Royal Decree 1337/1999 of 31 July regulating the transmission of information in the field of technical standards and regulations and regulations relating to information society services, has been observed.

PRELIMINARY TITLE

General provisions

Article 1. *Aim*.

The purpose of this Organic Law is to establish measures with the purpose of guaranteeing the protection of minors in digital environments.

Article 2. *Rights of minors*.

1. Minors have the right to be effectively protected against digital content that may impair their development.

2. Minors have the right to receive sufficient and necessary information in age-appropriate form and language about the use of technologies, as well as about their rights and the risks associated with the digital environment.

3. Minors have the right to access information, to freedom of expression, and to be heard.

4. Minors have the right to equal and effective access to devices, connection and training for the use of digital tools.

Article 3. *Purposes*.

The provisions of this Organic Law serve the following purposes:

a) Ensure respect for and compliance with the rights of children and adolescents in the digital environment, especially the rights to privacy, honour and self-image, the secrecy of communications and the protection of personal data and access to age-appropriate content.

b) Promote a balanced and responsible use of digital environments in order to ensure the proper development of the personality of minors and to preserve their dignity and fundamental rights.

c) Ensure that digital products and services take into account, by design and by default, the best interests of the child and integrate a gender and intersectional perspective.

d) Support the development of children's digital skills in the digital environment and the ability to assess online content and detect disinformation and abusive material.

e) Promote a safer digital environment and stimulate research in this area, taking into account the need for data disaggregated by sex.

f) Prevent sexual violence in the digital sphere, which includes the dissemination of acts of sexual violence through technological means, non-consensual pornography and sexual extortion, including advocacy of these behaviours.

TITLE I

Measures in the field of consumer and user protection

Article 4. *Obligations of manufacturers of digital terminal equipment with internet connection.*

1. This Article applies to digital terminal equipment that has an operating system and which has the ability to connect to the internet and through which content harmful to minors can be accessed, such as mobile phones, electronic tablets, smart TVs and personal computers.

2. Manufacturers of data terminal equipment referred to in the previous subparagraph shall provide information on their products, at least on the packaging and in the instruction book, user manual or user guide of the equipment, in a language that is accessible, inclusive and appropriate for all ages, risks arising from access to content harmful to the health and physical, mental and moral development of minors. They shall also provide information on data protection measures and risks related to privacy and security; the time recommended for using the products and services, appropriate to the age of the user; parental control systems; the risks to cognitive and emotional development and to sleep quality from prolonged use of such services. In any case, the adaptation of language and visual and audiovisual elements to the needs of people with disabilities and people with autism spectrum disorder shall be taken into account.

3. Manufacturers shall be obliged to ensure that in its operations system, the terminal equipment referred to in this Article includes a parental control functionality that allows its users to restrict or control the access of those persons to services, applications and content harmful to minors, the activation of which should occur by default at the time of the initial configuration of the terminal equipment. The inclusion of the functionality, its activation, configuration and update shall be free for the user.

Manufacturers shall ensure that the operating systems installed on their terminal equipment incorporate parental control functionality. The operating system provider shall, at the request of the manufacturer, ensure and certify to the manufacturer that the operating system intended to be installed on the terminal equipment incorporates the parental control functionality.

The personal data of minors collected or generated during the activation of this functionality may not be used in any case, even when the user acquires the age of majority, for commercial purposes, such as direct marketing, profiling and behavioural advertising.

4. Manufacturers must prove to importers, distributors and marketers that the devices supplied meet the requirements and conditions set out in the preceding subparagraphs. Importers,

distributors and marketers shall carry out actions to verify compliance with these requirements and conditions.

5. The State Secretariat for Telecommunications and Digital Infrastructures shall exercise the duties of surveillance, supervision and control of the requirements and conditions established in the previous subparagraphs, for which it shall exercise the powers of market surveillance and inspection established in Articles 83 and 103, respectively, of Law 11/2022, of 28 June, General Telecommunications and its implementing regulations, in particular Royal Decree 186/2016, of 6 May, regulating the electromagnetic compatibility of electrical and electronic equipment and Royal Decree 188/2016, of 6 May, approving the Regulation establishing the requirements for the marketing, putting into service and use of radio equipment, and regulating the procedure for conformity assessment, market surveillance and the sanctions regime for telecommunications equipment.

6. The following are classified as serious infringements:

a) The lack of information on their products referred to in paragraph 2 of this Article by manufacturers of digital terminal equipment.

b) The absence of parental control functionality in terminal equipment referred to in paragraph 3 of this Article by manufacturers of digital terminal equipment.

c) The erroneous design or manufacture of the terminal equipment or operating system that makes it impossible to activate the parental control functionality.

d) The activation, configuration and updating of the parental control functionality not free for the user.

e) The failure of the operating system provider to certify to the manufacturer that the operating system intended to be installed on the terminal equipment incorporates the parental control functionality on the digital terminal equipment.

f) The lack of accreditation by manufacturers to importers, distributors and marketers that the equipment and devices supplied meet the requirements and conditions established in this Article.

g) The lack of development by importers, distributors and marketers of actions to verify compliance with the requirements and conditions established in this Article.

Penalties imposed for any of the aforementioned infringements may lead to the withdrawal or recall of the equipment from the market or the prohibition or restriction of its placing on the market, until compliance with the requirements laid down in this Article has been achieved.

For the committing the offences referred to in the preceding subparagraphs, the offender shall be fined up to EUR 2 million.

The amount of the penalty imposed, within the limits indicated, shall be graduated taking into account, in addition to the provisions of Article 29 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, the following:

a) The severity of the offences previously committed by the subject to whom the penalty is imposed.

b) The damage caused.

c) Voluntary compliance with the precautionary measures that, where appropriate, are imposed in the sanctioning procedure.

d) Refusal or obstruction to provide the required information or documentation.

e) The cessation of the infringing activity, prior to or during the processing of the penalty proceedings.

f) Active and effective cooperation with the competent authority in detecting or proving the infringing activity.

The exercise of the sanctioning power corresponds to the head of the State Secretariat for Telecommunications and Digital Infrastructures. The instruction of the sanctioning files corresponds to the General Secretariat of Telecommunications and Management of Audiovisual Communication Services.

Once the sanctioning procedure has been initiated, the infringements referred to in this Article, in accordance with Article 56 of Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations, may lead to the adoption of the following precautionary measures:

a) Order the immediate cessation of any other allegedly infringing activity.

b) Order the withdrawal or recall from the market of telecommunications equipment which allegedly does not meet the requirements laid down in this Article.

Infringements shall be time-barred after 2 years.

Sanctions shall be time-barred after 2 years.

In the exercise of the sanctioning power, the common administrative procedure established in Law 39/2015, of 1 October, shall apply, although the period of resolution of the same shall be one year and the period of allegations shall be at least 15 working days.

7. The absence of requirements and conditions provided for in the second and third paragraphs of this Article shall be considered an objective lack of conformity of the products, for the purposes of Article 115 ter of the consolidated text of the General Law for the Protection of Consumers and Users and other complementary laws, adopted by Royal Legislative Decree 1/2007 of 16 November, for the exclusive purpose of conferring on consumers and users the rights provided for in that provision.

Article 5. *Regulation of access and activation of random reward mechanisms*.

1. Access to random reward mechanisms or their activation by minors is prohibited. For the purposes of this paragraph, a random reward mechanism shall be understood as a virtual functionality whose activation is carried out with legal tender or through a virtual object, such as a code, key, in-game currency, cryptocurrency or other element, acquired with money directly or indirectly; in which the result of such activation is random and consists of obtaining a virtual object that can be exchanged for money or other virtual objects. Where appropriate, regulations may determine the exceptional cases in which this prohibition may be relaxed, always guaranteeing the principle of protection of children that inspires this Law.

2. For the purpose of ensuring the effectiveness of this prohibition, the offer of random reward mechanisms can only be made when there are systems of age verification of users that prevent access or activation of these contents to minors.

Such systems shall ensure security, privacy and data protection, in particular in terms of data minimisation and purpose limitation.

TITLE II

Measures in the field of education

Article 6. *Training activities in pre-schools, primary schools, compulsory secondary schools and post-compulsory secondary schools*.

Educational administrations shall promote in pre-schools, primary, compulsory secondary and post-compulsory secondary schools, regardless of their ownership, the undertaking of activities aimed at improving digital competence in order to ensure the full integration of students in the digital society and the learning of a safe, healthy, sustainable, critical and responsible use of digital technologies for learning, work and participation in society, as well as the interaction with them and the prevention of sexual violence.

Educational administrations shall include, in their planning for the continuing training of teachers, of welfare and protection coordinators or coordinators, as well as administrative and service staff, training activities that facilitate teachers strategies to impact, inter alia, on security (including digital well-being and cybersecurity-related skills) and on issues related to digital citizenship, privacy and intellectual property.

In the ongoing training of university teaching staff and administration and service personnel, content aimed at training for the prevention, awareness and detection of digital sexual violence shall be incorporated.

Article 7. *Regulation of the use of devices in preschools, primary schools, compulsory secondary schools and post-compulsory secondary schools*.

The pre-schools, primary, compulsory secondary and post-compulsory secondary schools, regardless of their ownership, shall regulate, in accordance with the provisions approved for this purpose by the educational administrations and within the framework of the provisions of Article 124 of Organic Law 2/2006, of 3 May, on Education, the use of mobile and digital devices in classrooms, in extracurricular activities and in places and times of rest that take place under their supervision.

TITLE III

Measures in the field of protection of victims of gender-based violence and sexual violence

Article 8. *Victims of gender-based violence or sexual violence*.

Victims of gender-based violence or sexual violence facilitated by digital environments have the status of victims for the purposes of Organic Law 1/2004 of 28 December on comprehensive protection measures against gender-based violence and Organic Law 10/2022 of 6 September on comprehensive guarantees of sexual freedom, respectively.

Article 9. *Comprehensive social assistance services*.

Minors shall have the right to access information and guidance services and, where appropriate, immediate psychosocial care and legal advice, by telephone and online, 24 hours a day, every day of the year, as well as, where appropriate, to access reception services and psychological and social assistance for victims of gender-based violence and sexual violence and 24-hour crisis centres. All these services shall be essential services in nature.

TITLE IV

Measures in the field of health

Article 10. *Health promotion and prevention*.

1. Public administrations promoting studies on the use of information and communication technologies by minors shall take into account the principle of ‘health in all policies’ by providing information disaggregated by age, sex and other health determinants. The design of these studies should allow the acquisition of knowledge that contributes to the evaluation of the effects on their

health and development. Likewise, health administrations shall develop guidelines for the prevention and promotion of health in the use of information and communication technologies by minors.

2. The health administrations' programmes for the prevention and promotion of children's and young people's health shall include measures to identify problematic uses of these technologies and the early detection of changes in behaviour or physical, mental and emotional health problems resulting from inappropriate use. The individual and community actions included in these programs shall incorporate the biopsychosocial perspective and the integral development of the health of minors. In the early detection of situations of risk, special attention shall be paid to identifying those in which children and adolescents make priority use of the digital environment to establish peer relationships, or possible situations of violence through the digital environment.

3. Competent health administrations shall review actions to prevent addictive disorders for the inclusion of non-substance addictions related to the use of digital media.

4. The coordination of all public administrations and agents involved shall be promoted, especially of primary care services, specialised attention to mental health and addictive behaviours, social and educational services. In particular, health administrations shall promote the joint development with other public administrations of programs and referral circuits for the comprehensive approach of the detected health problems, including possible cases of violence through the digital environment, as well as maps of community resources and health assets that contribute to a healthy development of minors.

5. Training and awareness-raising on the health consequences and addressing the excessive use of information and communication technologies shall be facilitated for health professionals caring for this population.

Article 11. *Specialised care*.

The health administrations shall promote the establishment of specific health care procedures for minors with addictive behaviours without substance, in the specialised mental health care network, both in the Units of Attention to Addictive Behaviour, and in children's mental health centres. Specific health care procedures shall also be established for the comprehensive care of minors who are victims of violence through the digital environment.

TITLE V

Measures in the public sector

Article 12. *Participation, information and awareness-raising*.

1. Public administrations shall promote the guarantee of the rights of minors in the digital field from a preventive, feminist and integral perspective. as well as consultation and participation of children and youth.

To this end, they shall ensure the creation of quality digital content aimed at promoting healthy habits, good treatment, gender equality, democratic participation and access to different cultural formats.

2. Public administrations shall promote spaces for dialogue with children and adolescents to learn about their experience with information and communication technologies, as well as to design participatory initiatives related to cultural promotion in the digital environment and the fight against gender-based violence and sexual violence, in line with the provisions of Organic Law 1/2004 of 28 December on Comprehensive Protection Measures against Gender Violence and Organic Law 10/2022 of 6 September on the comprehensive guarantee of sexual freedom.

3. Public administrations shall, within the scope of their competences, develop awareness-raising, awareness-raising, prevention and information campaigns and activities on the risks associated with the inappropriate use of digital environments and devices, paying particular attention to the consumption of pornographic material and to the prevention, awareness-raising and detection of sexual violence.

4. Within the scope of their competences, public administrations shall promote the realisation of gender-sensitive studies and research on the prevalence of harassment and violence in their different domains in digital environments.

5. The General State Administration and the regional and local administrations shall promote the provision of meeting spaces for children and adolescents in which they can develop healthy leisure activities alternative to the use of information and communication technologies.

6. Public administrations and private sector entities shall use accessible, inclusive, non-sexist and adapted language in communications addressed to minors and in information addressed to or accessible to minors. The use of complex or confusing language shall be avoided, promoting transparent, understandable and accessible communication. In any case, the adaptation of language and visual elements to the needs of people with disabilities and people with autism spectrum disorder shall be taken into account.

Article 13. *Promotion of public-private collaboration, co-regulation and standardisation*.

The Ministry for Digital Transformation and the Civil Service, in collaboration with the competent Departments, shall encourage Internet access service providers from a fixed location to approve a code of conduct that establishes the mechanisms and parameters of secure configuration that they undertake to apply in the provision of their services in places of public access where public

services are provided and where their Internet access services are used, such as schools, institutes, libraries, civic centres, public offices, health centres, among others, to avoid access to inappropriate content by minors.

Article 14. *Guarantee of professional specialisation through training*.

1. Professional specialisation shall be ensured, at all levels of government, through compulsory initial training and continuous training to be provided to all professional sectors directly or indirectly involved in the prevention, detection, redress and response of non-substance addictions, gender-based violence or sexual violence, as well as in the care of child victims, and those related to perpetrators.

2. In application of this Organic Law, the Government, in collaboration with the autonomous communities, shall develop a framework program for training and retraining of these professional sectors that covers, in addition to the specific aspects related to each sector, gender stereotypes, trauma and its effects and responsibility in reducing secondary victimisation. Particular attention shall be paid to the situation and needs of victims of intersectional discrimination.

3. Public administrations shall encourage and promote specialised training in these sectors, with special emphasis on those professionals who have direct and regular contact with minors.

Article 15. *National Strategy on the Protection of Children and Adolescents in the Digital Environment*.

1. The Government in collaboration with the autonomous communities, the cities of Ceuta and Melilla, and local entities draw up a national strategy on the protection of children and adolescents in the digital environment, on a 3-yearly basis, with the aim of protecting the rights of children and adolescents in the digital environment. This Strategy shall be adopted by the Government.

2. The Strategy shall be drawn up in line with the State Strategy for the Rights of Children and Adolescents and the State Strategy to combat gender-based violence, and shall involve the Children's Observatory, third-sector bodies, civil society and, in particular, children and adolescents.

3. It shall be promoted and coordinated by the ministerial department responsible for children's policies.

4. The development of the Strategy shall involve the participation of children and adolescents through the State Council for the Participation of Children and Adolescents.

5. The National Strategy on the Protection of the Rights of Children and Adolescents in the Digital Environment shall promote:

a) The undertaking of activities aimed at education in digital citizenship and media literacy in order to ensure the full integration of children and youth in the digital society and promote the responsible use of digital media that favours the effective exercise of their rights in a safe and respectful digital environment.

Training in digital citizenship and media literacy shall be approached from a formative, preventive and social perspective, under the principles of equality, accessibility, intersectionality, respect, protection and guarantee of the rights of children and adolescents.

b) Dissemination of information to mothers, fathers or legal guardians, educational and health equipment on the appropriate use of digital devices and their impact on the development of children, with special attention to raising awareness of cyberbullying and cyber-aggressions, as well as parental control measures.

c) The use of secure digital devices and adequate prevention measures in educational and training spaces, especially when they are aimed at children and youth.

d) Neurobiological research, especially in relation to childhood and adolescence and the effects of technology on cognitive development; research on the use of pornography and its impact on children and adolescents; and research on the needs of children and adolescents in digital environments, addressing gender differences.

e) The creation of cooperative learning systems and public laboratories of digital culture.

f) Quality affective sexual education based on scientific evidence.

6. Biennially, the body responsible for driving the Strategy shall produce an evaluation report on its degree of compliance and effectiveness. This report, which must be submitted to the Council of Ministers, shall be drawn up in cooperation with the relevant ministries.

7. The strategy shall be reviewed every 3 years taking into account the rapidly evolving digital environment and research developments. To this end, a Follow-up Commission shall be set up with the participation of the Ministries of the Presidency, Justice and Relations with the Courts; Youth and Children; Health Education, Vocational Training and Sports; for the Digital Transformation and the Civil Service; of the Interior; Social Rights, Consumption and 2030 Agenda; Science, Innovation and Universities; and Equality, with the aim of promoting and monitoring the strategy.

Sole repealing provision. *Repeal of regulations*

Article 13(1) of the Regulation implementing Organic Law 15/1999 of 13 December on the protection of personal data, adopted by Royal Decree 1720/2007 of 21 December, is hereby repealed.

Likewise, any rules of equal or lower rank that oppose the provisions of this Organic Law are repealed.

First final provision. *Amendment of Organic Law 6/1985 of 1 July on the Judiciary*.

Article 90(5) of Organic Law 6/1985 of 1 July on the Judiciary is amended to read as follows:

> '5. It is also for the Central Administrative Courts to authorise, by order, the transfer of the data enabling the identification referred to in Article 8(2) of Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce, the material execution of the decisions adopted by the competent body to interrupt the provision of information society services or to remove content in application of the aforementioned Law 34/2002, of 11 July, as well as the limitation on the access of recipients to the intermediary service provided for in Article 51(3)(b) of 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.
>
> The Central Administrative Courts are likewise responsible for authorising the actions to be carried out by the competent audiovisual authority in accordance with Articles 93(4) and 164(1) of Law 13/2022 of 7 July on General Audiovisual Communication.'

Second final provision. *Amendment of Organic Law 10/1995 of 23 November on the Criminal Code*.

Organic Law 10/1995 of 23 November on the Criminal Code is amended as follows:

One. A new subparagraph (l) is added to Article 33(2) as follows:

> '(l) The prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space, for a period exceeding 5 years.'

Two. A new subparagraph (m) is added to Article 33(3) as follows:

> '(m) The prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space, for a period of 6 months to 5 years.'

Three. A new subparagraph (j) is added to Article 33(4) as follows:

> '(j) The prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space, for a period of 1 month to less than 6 months."

Four. A new subparagraph (k) is added to Article 39 as follows:

‘(K) The prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space.’

Five. Article 40(3) is amended to read as follows:

'(3) The penalty of deprivation of the right to reside or go to certain places shall be for a period of up to 10 years. The prohibition on approaching or communicating with the victim or their family members or other persons shall last from 1 month to 10 years. The prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space shall last from 1 month to 10 years.’

Six. Article 45 is amended to read as follows:

‘Article 45.

The special disqualification for profession, trade, industry or commerce or other activities, including those carried out or exploited in virtual spaces, whether paid or unpaid, or any other right, which must be specified in the verdict explicitly and with justification, deprives the person sentenced of the power to exercise them during the time of sentencing. The judicial authority may restrict the disqualification to certain activities or roles of the profession or trade, whether paid or unpaid, allowing, if possible, the exercise of those roles not directly related to the crime committed.’

Seven. Paragraph 4 is amended and a new paragraph 5 is added to Article 48 as follows:

'(4) The judge or court may agree that the control of the measures provided for in the previous paragraphs shall be carried out through those electronic means that allow it.

5. The prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space deprives the person sentenced of the power of access or communication through the internet, by telephone or any other information or communication technology during the time of the sentence, when they are directly related to the crime committed.

The content or scope of the prohibition shall be expressly specified and reasoned in the court decision.’

Eight. A new subparagraph 4 shall be added to Article 56(1) as follows:

‘4.º Prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space, when they are directly related to the crime committed.’

Nine. Paragraph 6 of Article 70(3) is amended to read as follows:

‘6.º In the case of deprivation of the right to reside or go to certain places, or the prohibition of access or communication through social networks, forums, communication platforms or any other place in the virtual space, the same penalty, with the clause that its maximum duration shall be 20 years.’

Ten. A new subparagraph numbered (10) is added to Article 83(1) as follows:

‘(10) Prohibition of access or communication through social networks, forums or virtual platforms when they are directly related to the crime committed.’

Eleven. A new Article 173 bis is added as follows:

‘Article 173(2).

A term of imprisonment of 1 to 2 years shall be imposed on anyone who, without the permission of the person concerned and with a view to impairing his or her moral integrity, disseminates, displays or cedes his or her body image or voice audio generated, modified or recreated by means of automated systems, software, algorithms, artificial intelligence or any other technology, in such a way that it appears real, simulating situations of sexual or seriously vexatious content.

The penalty shall be applied in its upper half if such deepfake material is disseminated through a means of social communication, through the internet or through the use of technologies, so that it becomes accessible to a large number of people in the virtual space.’

Twelve. A new subparagraph (e bis) is added to Article 181(5) as follows:

‘(e bis) Where, in order to facilitate the execution of the offence, the person responsible has used a fictitious or imaginary identity, or an age, sex or other personal conditions different from his own have been attributed.’

Thirteen. A new paragraph (3) is added to Article 182 as follows:

'(3) If, in order to facilitate the execution of the conduct defined in the previous paragraphs, the person responsible has used a fictitious or imaginary identity, or if an age, sex or other personal conditions different from his own have been attributed, the penalty shall be imposed in its upper half.’

Fourteen. Article 183 is amended to read as follows:

‘Article 183.

1. Any person who, through the internet, by telephone or any other information and communication technology, contacts a minor under the age of 16 and proposes to arrange a meeting with him or her in order to commit any of the offences described in Articles 181 and

189, provided that such a proposal is accompanied by material acts aimed at rapprochement, shall be punished by one to 3 years' imprisonment or a fine of 12 to 24 months, without prejudice to the penalties corresponding to the offences, if any, committed. Penalties shall be imposed in the upper half when the approach is obtained by coercion, intimidation, deception or using a fictitious or imaginary identity, or the aggressor is attributed an age, sex or other personal conditions different from his or her own.

2. Anyone who, through the internet, by telephone or any other information and communication technology, contacts a minor under the age of 16 and engages in acts aimed at deceiving him or her into providing pornographic material or showing him or her pornographic images depicting or appearing a minor shall be punished by imprisonment from 6 months to 2 years.

When the solicitation is carried out using a fictitious or imaginary identity, or attributing age, sex or other personal conditions different from their own, the penalty shall be imposed in its upper half.'

Fifteen. Article 185 is amended to read as follows:

'Article 185.

Anyone who executes or causes to be executed another person acts of obscene exposure to minors or persons with disabilities in need of special protection shall be punished by imprisonment from 6 months to 1 year or a fine from 12 to 24 months.

Where, in order to facilitate the execution of the conduct, the person responsible has used a false, fictitious or imaginary identity, or has attributed an age, sex or other personal conditions different from his or her own, the penalty shall be imposed in the upper half.'

Sixteen. Article 186 is amended to read as follows:

'Article 186.

Whoever knowingly and by any means sells, disseminates, displays or makes available pornographic material to minors or persons with disabilities in need of special protection shall be punished by imprisonment from 6 months to 1 year or a fine from 12 to 24 months.

Where, in order to facilitate the execution of the conduct, the person responsible has used a fictitious or imaginary identity, or an age, sex or other personal conditions different from his own have been attributed, the penalty shall be imposed in the upper half.'

Seventeen. Article 188(1) is amended to read as follows:

'(1) Anyone who induces, promotes, favours or facilitates the prostitution of a minor or a person with a disability in need of special protection, or thereby exploits or otherwise exploits

a minor or a person with a disability for these purposes, shall be punished by imprisonment of 2 to 5 years and a fine of 12 to 24 months.

If the victim is under the age of 16, the penalty shall be imprisonment from four to 8 years and a fine from 12 to 24 months.

Where, in order to facilitate the execution of the conduct, the person responsible has used a fictitious or imaginary identity, or an age, sex or other personal conditions different from his own have been attributed, the penalty shall be imposed in the upper half.'

Eighteen. Article 188(4) is amended to read as follows:

'(4) Anyone who requests, accepts or obtains, in return for remuneration or a promise, a sexual relationship with a minor or a person with a disability in need of special protection shall be punished by 1 to 4 years' imprisonment. If the minor has not reached the age of 16, a penalty of 2 to 6 years of imprisonment shall be imposed.

Where, in order to facilitate the execution of the conduct, the person responsible has used a fictitious or imaginary identity, or an age, sex or other personal conditions different from his own have been attributed, the penalty shall be imposed in the upper half.'

Nineteen. Article 189(3) is amended to read as follows:

'(3) If the acts referred to in point (a) of the first subparagraph of paragraph 1 have been committed with violence or intimidation, the penalty shall be higher than that provided for in the preceding paragraphs.

If, in order to facilitate the execution of the same acts referred to in point (a) of the first subparagraph of paragraph 1, the person responsible has used a fictitious or imaginary identity, or an age, sex or other personal conditions different from his own have been attributed, the penalty provided for in the preceding paragraphs shall be imposed in its upper half.'

Third final provision. *Amendments to Law 29/1998 of 13 July on Contentious-administrative Jurisdiction*

Law 29/1998, of 13 July, on Contentious-Administrative Jurisdiction, is amended as follows:

One. Article 9(2) is amended to read as follows:

'2. The Central Administrative Courts shall be responsible for the authorisation referred to in Article 8(2) of Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce, and the execution of the acts adopted by the body competent to interrupt the provision of information society services or to remove content in application of Law 34/2002, of 11 July, as well as the limitation on the access of recipients to the intermediary service

provided for in Article 51(3)(b) of 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.

The Central Administrative Courts are likewise responsible for authorising the actions to be carried out by the competent audiovisual authority in accordance with Articles 93(4) and 164(1) of Law 13/2022 of 7 July on General Audiovisual Communication.'

Two. Paragraph 2 is amended and a new paragraph 3 is added to Article 122 bis as follows:

'2. The implementation of measures to interrupt the provision of information society services or to remove content pursuant to Law 34/2002 of 11 July and to limit recipients' access to the intermediary service provided for in Article 51(3)(b) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 shall require prior judicial authorisation in all cases where the Constitution, the rules governing the respective rights and freedoms or those applicable to the different matters confer exclusive jurisdiction on the courts to intervene in the exercise of activities or rights, in accordance with the provisions of the following subparagraphs.

Once the measure has been agreed by the corresponding body, it shall request authorisation from the competent Court for its execution, referring to the possible affectation of the rights and freedoms guaranteed in the Constitution. The application shall be accompanied by the administrative file.

Within the non-extendible period of 2 days following receipt of the notification of the administrative decision and highlighting the file, the Court shall send the decision to the legal representative of the Administration, the Public Prosecutor's Office and the holders of the rights and freedoms affected or the person they designate as representative so that they can make written statements for a common period of 5 days.

If the written pleadings submitted prove to be new facts of relevance to the decision, the court may, having regard to the nature of the case, order an oral hearing or, failing that, if the written pleadings submitted do not prove to be new facts of relevance to the decision, the court shall give its decision within a period which may not be extended by 2 days by order. The decision taken may only authorise or refuse enforcement of the measure.

3. The provisions of the previous paragraph shall apply to the judicial authorisation of the actions to be carried out by the competent audiovisual authority in accordance with Articles 93(4) and 164(1) of Law 13/2022 of 7 July on General Audiovisual Communication.'

Fourth final provision. *Amendment of the consolidated text of the General Law for the Protection of Consumers and Users and other complementary laws, adopted by Royal Legislative Decree 1/2007 of 16 November*.

The consolidated text of the General Law for the Protection of Consumers and Users and other complementary laws, adopted by Royal Legislative Decree 1/2007 of 16 November, is amended as follows:

One. A new subparagraph (g) is added to Article 8(1) as follows:

> ‘(g) The protection of minors, as vulnerable consumers, in relation to digital goods or services.’

Two. A new subparagraph (t bis) is added to Article 47(1) as follows:

> ‘(t bis) The employer’s failure to comply with age verification and verification obligations in the procurement of goods or services intended for adults.’

Three. Article 48(2)(a) is amended to read as follows:

> ‘a) Infringements of Article 47(f), (g), (i), (k), (l), (m), (n), (ñ), (p), (q), (t) and (t bis) shall be classified as minor, unless they are considered serious in accordance with the third paragraph of this Article.’

Four. Article 62(1) is amended to read as follows:

> '(1) When contracting with consumers and users, their willingness to contract or, where appropriate, to terminate the contract must be unequivocally stated.
>
> Employers who offer goods or services intended for adults, either because of their sexual or violent content or because they pose a risk to physical health or the development of personality, must require, prior to hiring, the presentation or exhibition of an official document accrediting age or use any method of verification of age, effective and in accordance with the means through which the contract is to be carried out.’

Five. Article 98(2) is amended to read as follows:

> '2. If a distance contract to be concluded by electronic means entails payment obligations for the consumer and user, the trader shall make the information set out in Article 97(1)(a), (e), (p) and (q) known to the consumer and user in a clear and prominent manner, and just before the order is placed.
>
> The trader must ensure that the consumer and user, when placing the order, expressly confirms that he is aware that it implies an obligation to pay. If an order is placed by activating

a button or similar function, the button or similar function shall be labelled, in such a way as to be easily legible, only with the words ‘order with an obligation to pay’ or a similar unambiguous wording indicating that placing the order entails an obligation to pay the trader. Otherwise, the consumer and user shall not be bound by the contract or order.

Where the subject-matter of the distance contract is goods or services of their own or of others or, internally or externally, intended for persons of legal age, whether because of their sexual or violent content or because they pose a risk to physical health or the development of personality, prior to contracting the trader must require the presentation or exhibition of an official document accrediting the age or use any method of verifying the age, effective and in accordance with the means through which the contracting is to be carried out.’

Fifth final provision. *Amendment of Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights*.

Organic Law 3/2018, of 5 December, on the protection of personal data and the guarantee of digital rights, is amended as follows:

One. Article 7 is amended to read as follows:

'(1) The processing of the personal data of a minor may only be based on his or her consent when he or she is over 16 years of age.

Exceptions are made in cases where the law requires the assistance of the holders of parental authority or guardianship for the holding of the legal act or business in the context of which consent is sought for processing.

2. The processing of the data of children under 16 years of age, based on consent, shall only be lawful if it consists of the holder of parental authority or guardianship, with the scope determined by the holders of parental authority or guardianship.’

Two. Article 12.6 is amended to read as follows:

'(6) In any case, the holders of parental authority may exercise in the name and on behalf of children under 16 the rights of access, rectification, cancellation, opposition or any other rights that may correspond to them in the context of this Organic Law.

Sixth final provision. *Amendment of Law 13/2022 of 7 July on General Audiovisual Communication*

General Law 13/2022 of 7 July on Audiovisual Communication is amended as follows;

One. Two new paragraphs 8 and 9 are added to Article 3, renumbering the current paragraph 8 as paragraph 10:

‘(8) The audiovisual media service provider that, being established in a country that is not a member of the European Union or the European Economic Area, specifically directs its services to the Spanish market shall be obliged to comply with the provisions of Article 99(1), (2), (3) and (4) and Section 1a of Chapter IV of Title VI.

9. The provider of the video-sharing platform service that, being established in a country that is not a member of the European Union or the European Economic Area, specifically directs its services to the Spanish market, provided that this does not contravene the provisions of applicable international treaties or conventions, shall be obliged to comply with the provisions of Articles 88, 89, 90 and 91.’

Two. Article 42 is amended to read as follows:

‘Article 42. *Advertising of the ownership framework of audiovisual media service providers and video-sharing platform service providers.*

1. Providers of audiovisual media services and video-sharing platform service providers must make the following information accessible, in an easily understandable form and in electronic and reusable format, in the official language of the state and the official languages of the Autonomous Communities, on the respective corporate websites, without prejudice to their obligations under Law 34/2002 of 11 July 2002, Law 19/2013 of 9 December 2013, and the regulation in relation to non-financial information and diversity contained in the Commercial Code; in Royal Legislative Decree 1/2010 of 2 July 2010 approving the reworded text of the Share Capital Law, and Law 22/2015 of 20 July 2015 on the auditing of accounts:

a) name and registered office, contact details, including email, and whether or not it is profit-making or state-owned;

b) Establishment in Spain and competent audiovisual supervisory authority, including an easily recognisable and accessible link to the website of said authority so that users can notify possible infringements of audiovisual regulations.

c) natural or legal persons that ultimately hold editorial responsibility or authors of the editorial content;

d) natural or legal persons that own or hold significant interests within the meaning of Article 38;

2. Users of particular relevance using video-sharing platform services shall publish on their services in an easily recognisable and accessible way a link to the website of the audiovisual supervisory authority in order to allow users to report possible infringements of audiovisual regulations.’

Three. Paragraphs (e) and (f) of Article 89.1 are amended; which are worded as follows:

‘e) Establish and operate age verification systems for users with respect to content that may impair the physical, mental or moral development minors who, in any case, prevent their access to the most harmful audiovisual content, such as gratuitous violence or pornography.

Such systems shall ensure security, privacy and data protection, in particular in terms of data minimisation and purpose limitation.

f) Facilitate parental control systems controlled by the end user with respect to content that could harm the physical, mental or moral development of minors.

Four. Article 93(4) is amended to read as follows:

'(4) Failure to comply with the obligations laid down in Article 89(1)(e) shall constitute the offence referred to in Article 157(8), without prejudice to any criminal liability that may arise from such action. The National Commission on Markets and Competition may also adopt the measures provided for in Articles 8 and 11 of Law 34/2002 of 11 July, in accordance with the provisions of those Articles.

The implementation of the measures referred to in the preceding paragraph, including those requiring the cooperation of providers of intermediary services, shall require prior judicial authorisation in accordance with the procedure laid down in paragraph 2 of Article 122 bis of Law 29/1998 of 13 July, on Contentious-Administrative Jurisdiction. In the event that the provider repeats the definitively sanctioned infringing behaviour, provided that there is identity in the infringing service, the execution of the measures contained in the previous paragraph shall not require judicial authorisation, from the second time that the recidivism occurs.’

Five. Article 94(1) is amended to read as follows:

'(1) Users of particular relevance using video-sharing platform services shall be considered as audiovisual media service providers for the purposes of compliance with the principles set out in Articles 4, 6, 7(1), 10, 12, 14, 15; the obligation laid down in Article 42(2) and the obligations for the protection of minors as laid down in Article 99(1), (2), (3) and (4). Such users shall also comply with Sections 1 and 2 of Chapter IV of Title VI when placing on the market, selling or organising commercial communications accompanying or embedded in their audiovisual content.

Users of particular relevance shall take appropriate measures to comply with these obligations and shall use the mechanisms made available to them by the provider of the video-sharing platform service, in particular those laid down in Articles 89(1)(d) and 91(2)(b).’

Six. Article 99(3) and (4) are amended and phrased as follows:

'(3) Conditional access linear television audiovisual media services have the following obligations for the protection of minors from harmful content:

a) Comply with the co-regulation code provided for in Article 98(2);

b) Provide parental control mechanisms.

c) Establish and operate age verification systems for users with respect to content that may harm the physical, mental or moral development of minors that, in any case, prevent their access to the most harmful audiovisual content, such as gratuitous violence or pornography. Such systems shall ensure security, privacy and data protection, in particular in terms of data minimisation and purpose limitation.

4. The on-demand television audiovisual media service has the following obligations for the protection of minors from harmful content:

a) Include audiovisual programmes and content that may involve scenes of pornography or gratuitous violence in separate catalogues.

b) Comply with the co-regulation code provided for in Article 98(2);

c) Provide parental control mechanisms.

d) Establish and operate age verification systems for users with respect to content that may harm the physical, mental or moral development of minors that, in any case, prevent their access to the most harmful audiovisual content, such as gratuitous violence or pornography. Such systems shall ensure security, privacy and data protection, in particular as regards data minimisation and purpose limitation.'

Seven. A new subparagraph (b bis) is added to Article 155(2) as follows:

'(b bis) Television audiovisual media service providers and video-sharing platform service providers established in a country that is not a member of the European Union or the European Economic Area that specifically target their services to the Spanish market in accordance with Articles 3(8) and 3(9).'

Eight. Article 160(1)(c) is amended to read as follows:

'(c) The penalties provided for in points (a) and (b) of this paragraph may also include one of the following ancillary sanctions:

1.º Revoking the licence to provide audiovisual media services and consequently ceasing to provide the service when the provider has committed the very serious offence referred to in Article 157(6) and (7).

2.º The cessation of broadcasting, and the provisional sealing of equipment and installations used to perform the emission when the very serious infringement provided for in Article 157(4) and (5) has been committed.

3.º The cessation of the provision of the service and the loss of the status of provider acquired through prior notification, for a maximum period of one year, when the very serious infringement provided for in Article 157(13) and (14) has been committed.

4.º The cessation of the provision of the service by the provider of the video-sharing platform service, for a maximum period of one year, when the very serious infringement provided for in Article 157(8) has been committed.'

Nine. Article 164(1) is amended to read as follows:

'(1) Once the sanctioning procedure has been initiated for any of the infringements established in Articles 157, 158 and 159, provisional measures may be adopted which, in accordance with Article 56 of Law 39/2015, of 1 October, may consist of the following:

a) Ordering the immediate cessation of any allegedly infringing activity.

b) Confirming or amending the provisional measures adopted pursuant to the previous Article. These provisional measures shall be valid for a maximum of 3 months and may be extended for a further period of up to 3 months.

c) Provisionally suspending the effectiveness of the licence and the provisional closure of the facilities, in the event of very serious infringements referenced in Article 157(5) and (6).

d) In the case of very serious infringements typified in paragraphs 8 and 14 of Article 157, the measures provided for in Articles 8 and 11 of Law 34/2002, of 11 July, may be adopted in accordance with the provisions of said articles, including the interruption of the infringing service and the removal of data. The execution of the measures, including those that require the collaboration of providers of intermediary services, shall require prior judicial authorization in accordance with the procedure regulated in paragraph 2 of Article 122 bis of Law 29/1998, of 13 July, on Contentious-Administrative Jurisdiction. In the event that the provider repeats the infringing conduct, sanctioned definitively, provided that there is identity in the infringing service, the execution of the measures shall not require judicial authorisation, from the second time that the recidivism occurs.'

Seventh final provision. *Jurisdiction*.

This Organic Law is issued on a basic basis under the provisions of Article 149(1). (1) and (13), which confers on the State exclusive competence in the regulation of the basic conditions that guarantee the equality of all Spaniards in the exercise of rights and in the fulfilment of constitutional duties; and of bases and coordination of the general planning of the economic activity.

More specifically:

The contents of Title II constitute basic rules for the development of Article 27 of the Constitution, in accordance with the provisions of Article 149(1)(30) of the Spanish Constitution.

Title IV is provided by virtue of the competence of the State in matters of bases and general coordination of health, provided for in Article 149(1)(16) of the Spanish Constitution.

The first, second and third final provisions are issued under the jurisdiction in matters of criminal and procedural legislation, which Article 149(1)(6) of the Spanish Constitution attributes to the State.

The fourth final provision is also issued under the jurisdiction in matters of civil law, provided for in Article 149(1)(8) of the Constitution.

In the sixth final provision amending Law 13/2022 of 7 July on General Audiovisual Communication, the amendments to Articles 42 and 160 thereof are issued in accordance with Article 149(1)(27) of the Spanish Constitution, which confers on the State exclusive competence in relation to the basic rules of the press, radio and television system and, in general, of all social media, without prejudice to the powers of development and enforcement that correspond to the Autonomous Communities. The rest of its contents are dictated under the exclusive competence of the State in matters of telecommunications attributed to it by Article 149(1)(21) of the Spanish Constitution.

Eighth final provision *Nature of Organic Law*.

The first, second and fifth final provisions have the character of an Organic Law. The rest of the precepts have the nature of ordinary law.

Ninth final provision. *Regulatory implementation*.

1. The Government is empowered to make the necessary provisions for the implementation of the provisions of this Organic Law.

2. Within 6 months of the entry into force of the obligations provided for in Article 4, the Government shall, by Royal Decree, determine the information to be provided by manufacturers, the format in which it is to be provided and a specification of the risks to be reported on.

Tenth final provision. *Entry into force*.

This Organic Law shall enter into force on the twentieth day following that of its publication in the Official State Gazette.

However, the obligations provided for in Article 4 shall enter into force 1 year after the publication of this Organic Law in the Official State Gazette.s

TO BE SUBMITTED TO THE COUNCIL OF MINISTERS

Madrid, on 2024

Minister for the Prime Minister’s

Office, Justice and Relations with Parliament	THE MINISTER FOR YOUTH AND CHILDREN
Félix Bolaños García	Sira Abed Rego
THE MINISTER FOR DIGITAL TRANSFORMATION AND PUBLIC SERVICE	THE MINISTER FOR SOCIAL RIGHTS, CONSUMPTION AND AGENDA 2030
Óscar López Águeda	Pablo Bustinduy Amador