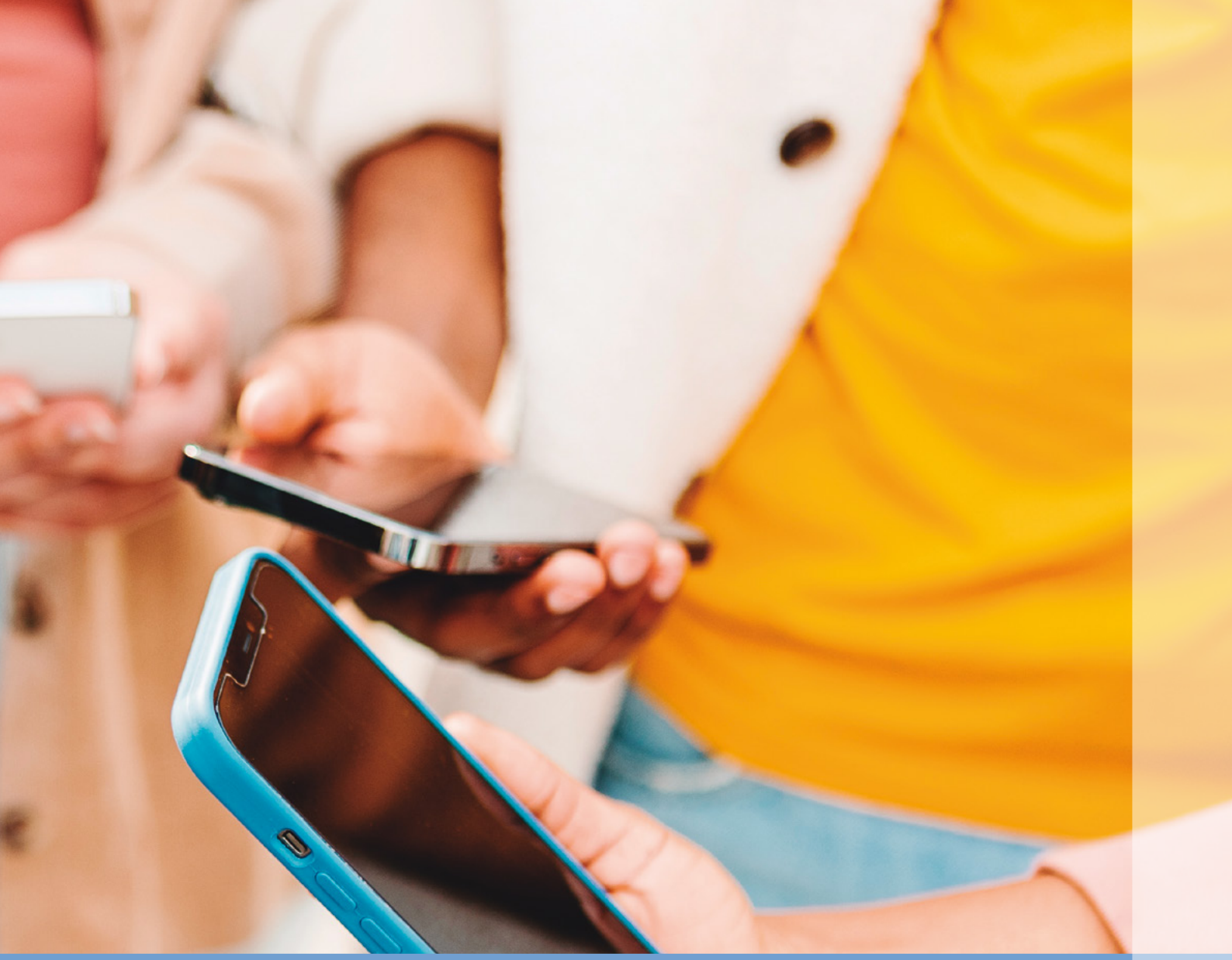


Digital protection for children and teenagers

Specific recommendations and proposals for authorities, operators, developers and families

Col·legi de Metges de Barcelona

Members of the Expert Group promoted by the CoMB: Rosa Calvo, Jordi Camós, Cesc Gummà, Xavier Ibarz, Marc Masip, Lluís Mulero, Silvia Ramón-Cortés, Marc Ferreira, Tomàs Moré, Montse Sánchez, Jordi Royo, Toni Calvo and Natàlia Raguer.

February 2024

Contents

1. Background 5
2. Reasons and clinical basis 6
3. List of proposals and recommendations 9
   - 3.1. For public authorities 9
     - Regulations 9
     - Regulations for telecommunications services 11
     - Education 13
     - Health care 14
   - 3.2. For telecommunications operators 14
     - Child SIM 15
     - Child Wi-Fi Mode 16
     - Providing DNS services with content filtering 18
     - Device configuration services for children 18
   - 3.3. For the developers of online platforms and search engines 18
   - 3.4. For families 21
4. Next steps for the CoMB 25
5. Appendices 27
   - 5.1. Appendix I: Bibliography 27
   - 5.2. Appendix II: Definitions and acronyms 28
   - 5.3. Appendix III: Regulatory framework 29
   - 5.4. Appendix IV: Members of the Expert Group promoted by the CoMB 30

1

Background

The Barcelona Medical Association is well aware of the public debate begun this year by groups of families regarding the use of mobile phones in schools and colleges, and the debate on the consequences of overexposure to screens and children's early exposure to certain content and applications.

On 13 March 2023, the conference "Mobile phones and the internet: a serious risk to the health of children and teenagers" was held at the CoMB headquarters[1] with the participation of health professionals in the fields of paediatrics and clinical psychology. There, the multiple effects on the health of children and teenagers caused by screens was made clear.

As a result, on 18 May 2023, CoMB established a multidisciplinary working group with the aim of providing medical insight into the public debate, as well as identifying specific, applicable proposals for action aimed at the different economic and social agents involved.

This document is the first compilation of recommendations and requests for action emerging from the CoMB working group and aimed at public authorities, telecommunications operators, application developers and families.

Given the serious consequences of overexposure to screens, we believe CoMB must take up a position in line with the institution's statutory principles, values and objectives (Art. 4 point D)[2] in favour of working with public authorities and other institutions to achieve the right to health protection.

The new regulatory framework promoted by the European Union, with the roll-out of the Digital Act, as well as the Spanish Audiovisual Communication Act, which establishes new obligations for technology agents (including so-called influencers), give the CoMB the opportunity to actively protect patients' right to health.

As a result, this document details a proposed action plan for CoMB on how to uphold those rights.

[1] https://youtu.be/kyWAy_z5peo?si=Ri4Hbsodlm8Et8bm
[2] https://www.comb.cat/pdf/estatuts.pdf

2

Reasons and clinical basis

Childhood and adolescence are critical periods of brain development when young people require special protection and care.

Exposure to social media, the lack of protection for children against certain functions aimed at increasing usage time, and access to potentially dangerous content pose a risk to children's development in terms of their physical and mental health.

Cognitive and social development

A meta-analysis published in JAMA Pediatrics[3] found that young children who spend more time in front of screens are more likely to have delayed language development and fewer language skills. The results of the analysis of these 42 studies, with more than 18,900 participants, support the recommendation to limit screen time, select high-quality content and watch it together with the child. Other cognitive problems linked to overexposure to screens in children were described more than 20 years ago, such as reduced attention span,[4] as well as an increased risk of aggressive behaviour in this population.[5]

There is also sufficient evidence[6] on how excessive screen use can reduce opportunities for face-to-face interaction crucial to the development of social and emotional skills in children.

Mental health

In a recent systematic review published in the BMJ,[7] social media use is associated with increased health risk behaviours in adolescents (alcohol, drug, tobacco consumption; risky sexual behaviour; antisocial behaviour; multiple risk behaviours; and gambling).

[3] Madigan, S., Browne, D., Racine, N., Mori, C., & Tough, S. "Association Between Screen Time and Children's Performance on a Developmental Screening Test." JAMA Pediatrics, 2019. DOI: 10.1001/jamapediatrics.2019.2078.
[4] Christakis, D. A., & Zimmerman, F. J. "Early television exposure and subsequent attentional problems in children." Journal of Developmental & Behavioral Pediatrics, 2004. DOI: 10.1097/00004703-200404000-00005.
[5] Ferguson, C. J. "The influence of television and video game use on attention and school problems: A multivariate analysis with other risk factors controlled." Pediatrics, 2011. DOI: 10.1542/peds.2010-1154.
[6] Hutton, J. S., Horowitz-Kraus, T., Mendelsohn, A. L., DeWitt, T., & Holland, S. K. "Associations Between Screen-Based Media Use and Brain White Matter Integrity in Preschool-Aged Children." Pediatrics, 2019. DOI: 10.1542/peds.2018-1446.
[7] BMJ 2023;383:e073552. http://dx.doi.org/10.1136/bmj-2022-073552
[8] Kross, E., Verduyn, P., Demiralp, E., Park, J., Lee, D. S., Lin, N., ... & Ybarra, M. "Social Media Use and Perceived Social Isolation Among Young Adults in the U.S." Journal of Adolescent Health, 2016. DOI: 10.1016/j.jadohealth.2016.12.005.
[9] Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. "Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time." Clinical Psychological Science, 2017. DOI: 10.1177/2167702617723376.

Previous studies have already reported the impact on the self-esteem of adolescents who make intensive use of social networks[8] and the increased risk of cyberbullying. In general, the amount of time a teenager spends on social media and electronic devices would be proportional to an increase in anxious and depressive symptoms, including thoughts of and attempts at suicide.[9]

The impact of social media on the development and evolution of eating disorders is a topic of growing concern. Most eating disorders begin between the ages of 14 and 16, and in recent years there is even evidence of a trend towards an earlier age of onset. Adolescence is a stage when the need to establish and nurture relationships outside the family environment becomes especially important, as well as the need to feel accepted by this broader social environment. While social media provide new and different opportunities for socialisation for young people and teenagers, they are also a potentially dangerous environment. It is in this context that concern for image becomes particularly important.

Social media can serve as a space for promoting ideals of thinness that make teenagers' relationships with their own bodies more difficult. They are spaces that encourage concern about weight and image, not only through peer comparison but also through upward comparison (influencers and role models). Added to this is the possibility of manipulating images using filters and retouching, which allows them to be made more attractive and closer to ideal models. This encourages teenagers to follow ideal models and strengthens the belief that they could be achievable.

In a meta-analysis of studies published between 2011 and 2021, the promotion of concern about weight and image and the objectification of the body arising from the practice of uploading, viewing and comparing photographs with the peer group are highlighted as negative aspects linked to the use of social media.[10]

Another study, published in 2024 in the Journal of Eating Disorders and conducted with a sample of more than 1,558 teenagers, found a clear association between the use of social media involving images and/or videos and eating disorders, apparently conveyed through the internalisation of body ideals (thinness more frequent among women, muscularity more frequent among men), and the perceived pressure to achieve these ideals.[11]

Although the risk is higher among the female population, there is evidence that the greater objectification of the body is an effect also present in men. Along these lines, in their 2022 study on the relationship between Instagram use and body esteem in men, Boursier and Goia found that greater Instagram use is related to greater objectification of the body, as it makes it easier to scrutinise the body and internalise images that negatively affect body self-image.[12]

[10] An Sist Sanit Navar 2022; 45(2): e1009 https://doi.org/10.23938/ASSN1009
[11] Dahlgren, C.L., Sundgot-Borgen, C., Kvalem, I.L. et al. Further evidence of the association between social media use, eating disorder pathology and appearance ideals and pressure: a cross-sectional study in Norwegian adolescents. J Eat Disord 12, 34 (2024). https://doi.org/10.1186/s40337-024-00992-3
[12] Boursier V, Gioia F. Which are the Effects of Body-Objectification and Instagram-Related Practices on Male Body Esteem? A Cross-Sectional Study. Clin Neuropsychiatry. 2022 Feb;19(1):8-19. doi: 10.36131/cnfioritieditore20220103. PMID: 35401765; PMCID: PMC8969847.

There is also evidence that the use of social media affects the cognition and actual eating behaviour of young people.[13]

Finally, it is important to mention the existence of multiple sources of content that promote unhealthy and extreme eating behaviours (pro-anorexia, pro-bulimia profiles) and their association with worse development in eating disorders.

Physical health

- **Sedentary lifestyle, obesity and sleep problems**

  Already in 2015, in a meta-analysis[14] a significant relationship was found between screen time and childhood obesity due to sedentary lifestyles and increased consumption of unhealthy foods during screen time.[15] It has also been shown[16] that screen use before bedtime is associated with children sleeping less well for less time, with consequences for learning and health that are already well known.[17]

- **Eyestrain and myopia**

  Children who use screens for long periods experience more symptoms of digital eye strain, such as dry eyes and eye discomfort. An association has also been demonstrated in children between long periods spent doing close activities (including screen use) and an increased risk of developing myopia.[18]

[13] BWilksch SM, O'Shea A, Ho P, Byrne S, Wade TD. The relationship between social media use and disordered eating in young adolescents. Int J Eat Disord. 2019;1–11
[14] Suchert, V., Hanewinkel, R., & Isensee, B. "Sedentary behavior, depressed affect, and indicators of mental well-being in school-aged children and adolescents: A systematic review and meta-analysis," Obesity Reviews, 2015. DOI: 10.1111/obr.12251.
[15] Stiglic, N., & Viner, R. M. "Effects of screentime on the health and well-being of children and adolescents: a systematic review of reviews," International Journal of Behavioral Nutrition and Physical Activity, 2019. DOI: 10.1186/s12966-018-0585-9.
[16] Hale, L., & Guan, S. "Screen time and sleep among school-aged children and adolescents: a systematic literature review," Journal of Pediatrics, 2014. DOI: 10.1016/j.jpeds.2014.01.036.
[17] Carter, B., Rees, P., Hale, L., Bhattacharjee, D., & Paradkar, M. S. "Association between portable screen-based media device access or use and sleep outcomes: a systematic review and meta-analysis," Sleep Medicine Reviews, 2016. DOI: 10.1016/j.smrv.2016.10.006.
[18] Huang, H. M., Chang, D. S., & Wu, P. C. "The association between near work activities and myopia in children: a systematic review and meta-analysis," Investigative Ophthalmology & Visual Science, 2015. DOI: 10.1167/iovs.15-17220.

3 List of proposals and recommendations

3.1. For public authorities

Regulations

- Without prejudice to the roll-out of the European eIDAS-2 regulations[19] on digital identity that should enable secure, anonymous digital authentication systems for citizens by 2030, public authorities should **urgently roll out effective systems and/or strategies to verify whether people are of legal age**[20] that would allow compliance with the obligations the Spanish General Act on Audiovisual Communication (LGCA) imposes on video sharing platforms (VSPs) and ensure the protection of children against potentially harmful content.

  In this regard, we should highlight the Spanish Data Protection Agency's (AEPD) initiative in the launch on 13 December 2023 of three PoCs (proofs of concept), as well as a set of principles for age verification. The CoMB supports the AEPD initiative and we call for plans to roll it out to be speeded up if the PoC's conclusions are valid.[21]

  PoC1 Video: https://www.youtube.com/watch?v=kv9XlJ80JfY&list=PLUjcI9KR6XD CXE2bdG7azbgWhq4rH31RY&index=1
  PoC2 Video: https://www.youtube.com/watch?v=aOVpKbUo1d0&list=PLUjcI9KR6X DCXE2bdG7azbgWhq4rH31RY&index=2
  PoC3 Video: https://www.youtube.com/watch?v=k3X0JFb6RJg&list=PLUjcI9KR6X DCXE2bdG7azbgWhq4rH31RY&index=3

- Expanding the scope of age verification systems[22] to other digital services beyond VSPs (e.g.: online gaming, social media, app stores, marketplaces, instant messaging apps, etc.).

[19] Normativa que actualitza el vigent reglament europeu "eIDAS".
[20] En línia amb la consulta pública de la CMNC vigent fins al 31 de gener de 2024 "Sobre els criteris per garantir la idoneitat dels sistemes de verificació d'edat dels Serveis d'Intercanvi de Vídeo a través de plataformes sobre continguts perjudicials per al menor".
[21] https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-presenta-sistema-verificacion-edad-para-proteger-a-menores-de-edad
[22] Inclosos a l'Art. 89 punt 1e. de la Llei 13/2022, de 7 de juliol, General de Comunicació Audiovisual.

- Prioritising the assignment and appointment of "competent authorities" responsible for overseeing technology companies and implementing the Digital Act regulations.

  As each member State can assign one or more "competent authorities", the possible dovetailing of powers so that the regional authorities can appoint their own competent authorities must also be considered.

- Among the "competent authorities", appointing the "Digital Services Coordinator" of the Member State, who will be part of the European Board for Digital Services.

- Accrediting authorised researchers[23] to carry out studies on systemic risk detection systems, as well as assessing the impact of the risk mitigation measures they are required to implement.

  These authorised researchers are the ones who can actually confirm the degree of compliance with preventive measures against risks to users (including the protection of public health and children), thanks to the access to the platforms' logarithmic systems granted to them by law. They therefore become a key tool when it comes to monitoring digital service providers and their response to warnings and complaints from users.

- Establishing a network of reliable whistleblowers[24] to bring the rights and protections granted by the Digital Act closer to citizens, because:
  - They make it easier for users to warn and complain.
  - They have priority attention from the platforms to resolve warnings and complaints.
  - Their actions in relation to each platform are recorded for auditing, transparency and oversight purposes by the Commission, and they are one of the necessary elements prior to developing a framework of penalties.

- Requesting the Government of Catalonia to establish "reliable whistleblowers" in the areas of government where there is more direct contact with child users, such as:
  - The Department of Education, for referring incidents in the use of digital services that can be identified in schools and colleges.
  - Department of Health, for referring incidents in the use of digital services that healthcare and mental health professionals identify among their patients.

    The reliable whistleblower at the Department of Health can become the reference point for health professionals when they identify risk situations for patients' physical and mental health linked to the use of digital services.

[23] D'acord amb els requisits establerts a l'Art. 40 punt 8 de la Digital Act.
[24] D'acord amb l'Art. 22 del Digital Act, la condició d'alertador fiable l'atorga el Coordinador de Serveis Digitals prèvia sol·licitud de qualsevol entitat que demostri disposar de les condicions establertes.

  - The Catalan Cybersecurity Agency, as a leading institution for citizens in the field of digital security and outreach and awareness programmes (e.g.: "safe internet" programme).

Telecommunications service regulators

- Prompting and encouraging operators that offer connectivity services to households/families to provide parental protection tools.

  See detailed draft proposals for telecommunications operators ("Children's SIM", "Children's Wi-Fi Mode", DNS Protection, configuration services).

- Promoting and encouraging the incorporation of the "Child" parameter[25] when providing their services and making this parameter accessible to third parties (e.g. stores, applications, apps, games, etc.) as a delegated age verification system.

- Promoting changes in the system and procedure for coding and categorising applications/games that developers use:
  - Monitoring the protocols with which the developer requests coding (self-declaration form).
  - Updating the "PEGI CONTENT DESCRIPTOR" codes[26] to incorporate codes that illustrate the existence of "dopamine triggers"[27] (loot boxes, social recognition-reinforcement elements, etc.).
  - Incorporating a coding equivalent to the "nutri-score"[28] that provides users with an easy interpretation of the potential addictive level of the application/game, by incorporating elements such as:
    - Whether the developer's business model is based on monetising the user's usage time.
    - Existence of elements of social reinforcement.
    - Existence of value reserve-recognition functions linked to user behaviour within the App (e.g.: coins, add-ons, badges, etc.).
    - Existence of algorithms that adapt the application to the user's tastes to increase their usage and connection time (e.g.: content proposal algorithm in the timeline, etc.).
    - Existence of infinite functionalities (infinite scrolling, autoplay, etc.).
    - Existence of self-limitation and/or parental protection tools.

- Promoting warning and complaint functions in application distribution platforms (App Store, Google Play) that allow users to report apps with incomplete and/or inaccurate coding for review.

[25] Òptimament la data de naixement de l'usuari a fi i efecte que a mesura que el menor vagi fent-se gran els filtres d'accés s'actualitzin automàticament.
[26] PEGI Contento descriptors: Codis que alerten l'usuari de contingut violent, llenguatge inapropiat, contingut sexual, apostes, drogues, contingut discriminatori... https://pegi.info/what-do-the-labels-mean
[27] *Dopamine triggers*: funcionalitats incorporades a les apps específicament per fer les funcions de disparadors de dopamines al cervell de l'usuari i que poden desenvolupar comportaments addictius.
[28] Nutri-score: https://es.wikipedia.org/wiki/Nutriscore

- Universalising access to parental protection tools by requiring telecommunications operators to offer parental protection and content filtering tools (DNS with parental protection) by default, both in new contracts (provided there are children in the home) and in already active contracts (at the customer's request).
- Promoting the "children by default" principle on digital platforms, so that the functions of the application are limited unless the user proves they are of legal age.
- Alongside the implementation of eIDAS-2 within the EU framework29 and the aforementioned PoCs promoted by the AEPD, promoting alternative tools and protocols allowing age verification, some of which the CMNC already highlights in its "Public consultation on the criteria for ensuring the suitability of age verification systems in video sharing services using platforms with content harmful to children":[30]
    - By bank card: requiring validation by a bank that the user has access to a bank card (rarely accessible to children under 12 years of age) as a prerequisite.
    - Independent age verification bodies: a third party not linked to the provision of the service verifies that the user is of legal age.
    - Verification via social support: to be considered "of legal age", the user must ask third parties (with verified legal age) to confirm to the platform that they are of legal age.
    - Age estimating technologies using video selfies: using AI tools that are able to identify the age ranges of users (e.g. Instagram has incorporated the Yoti technology solution in the testing phase in some countries[31] which allows the user's age to be established using a video selfie).
    - Self-exclusion register, equivalent to the General Register of Gambling Access Prohibitions (RGIAJ),[32] which allows users to register remotely (as individuals or as representatives of a child). Platforms should be required to confirm whether the requesting user is included in the self-exclusion register.
    - 2FA "Of Age": where the user provides a unique identifier to an independent verification service[33] which confirms whether the user is listed in a pre-existing repository (e.g.: Child SIM user register, self-exclusion register). If the identifier is not included in the repository, it enables access.
    - Other verification methods and systems certified by international bodies (e.g.: https://accscheme.com/registry/).

29 Proposta eIDAS-2 https://eur-lex.europa.eu/legal- content/ES/TXT/HTML/?uri=CELEX:52021PC0281
30 https://www.cnmc.es/consultas-publicas/audiovisual/verificacion-edad-contenidos-menor
31 https://www.yoti.com/.
32 Web registre de la direcció general d'ordenació del joc https://ordenacionjuego.es/es/rgiaj
33 Fa un procediment equivalent a l'autentificació delegada OAuth.

Education

- Members of the Expert Group promoted by the CoMB subscribes to and supports the ban on the use of smartphones in infant and primary schools by the Government of Catalonia's Department of Education.
- The "General framework governing the use of mobile phones"[34] to be developed by the Government of Catalonia's Department of Education, at the suggestion of the School Council of Catalonia (CEC), should include, among other initiatives.
    - Promoting and establishing "Mobile-Phone-Free Spaces" in secondary schools and post-compulsory education centres to strengthen socialisation among students. These spaces should include areas such as:
        - The dining room.
        - Leisure-play areas/playground.
        - Communal areas for pupils at the Infant and Primary education stages (where applicable).
        - Non-teaching educational activities (outings, etc.).
    - Promoting initiatives within the educational community aimed at reducing social pressure around the age of adoption of the first smartphone, following international best practices such as Wait Until 8th[35] (equivalent to "wait until 13-14"). This includes more than 50,000 families who have made the commitment not to give a smartphone to their children until they are 13-14 years old.

      This commitment DOES allow minors to use mobile phones without a smartphone's capacity for installing applications, accessing social networks, using internet browsers, etc.
    - Implementing a compulsory educational programme from an early age that addresses digital literacy, awareness of the responsible use of technology, and the identification of online risks. Including specific subjects on internet safety, digital ethics, consequences of misuse and skills in discerning appropriate content.
    - Establishing warning and complaint protocols that provide pupils with access to the bodies established by the Digital Act (network of reliable whistleblowers and/or Digital Services Coordinator of the Member State) and allow the protection of children's interests against:
        - Incidents involving the exposure of child users to potentially dangerous content (illegal content).
        - Complaints about illegal and non-consensual sharing of private images on a social network.
        - Online harassment and cyber extortion on a social network.
        - Exposure to potentially harmful content.
        - Incidents involving content moderation tools used by social networks.

34 Proposta eIDAS-2 https://eur-lex.europa.eu/legal- content/ES/TXT/HTML/?uri=CELEX:52021PC0281
35 https://www.cnmc.es/consultas-publicas/audiovisual/verificacion-edad-contenidos-menor

- Adapting the school's infrastructure to:
  - Establish filtering of potentially dangerous content by implementing:
    - A firewall.
    - DNS with content filters.

Health care

- Incorporating questionnaires into paediatric check-ups to detect risk behaviours (overexposure, early exposure).
- Publicising the risks, tools and recommendations for screen use by children among the medical community.
- Making the paediatrician a reference point for families in relation to decisions about child screen use.
- Publicising visual health habits and prevention measures regarding the risks of early exposure and overexposure.
- Establishing warning and complaint protocols providing patient access to the bodies established by the Digital Act (network of reliable whistleblowers and/or Digital Services Coordinator of the Member State) and allowing the protection of children's interests against:
  - Incidents involving the exposure of child users to potentially dangerous content (illegal content).
  - Complaints about illegal and non-consensual sharing of private images on a social network.
  - Online harassment and cyber extortion on a social network.
  - Exposure to potentially harmful content.
  - Incidents involving content moderation tools used by social networks.

3.2. For telecommunications operators

Telecommunications operators are **necessary agents** for users to access online services. They provide and activate the technology needed to provide users with connectivity.

In the process of activating a new user/customer, operators are required by the regulatory authorities of the telecommunications market to identify the users of their services through KYC processes[36] which they already have implemented in their routine operations.

These KYC processes allow a service (IP, SIM, etc.) to be uniquely identified with the responsible user/client (whether that is an individual or an organisation).

[36] KYC. Know Your Customer, procediments pels quals l'operador identifica l'usuari dels seus serveis.

This KYC process could potentially become proof of age, as suggested by the CMNC in the "Public consultation on criteria to ensure the suitability of age verification systems".[37] Although this is neither a complete nor an exhaustive solution, it would be applicable in cases where the user voluntarily states that they are underage (e.g. family/guardians when registering a mobile phone line for a child).

In terms of service provision, telecommunications operators provide the hardware and software elements necessary for users to access the network. These are capable of filtering content and managing access windows.

The CoMB calls on telecom operators to be part of the solution and cooperate in favour of public health by voluntarily implementing self-limiting and self-regulating solutions.

The CoMB invites operators to roll out services such as:

Child SIM

This provides families with a mobile phone service contracting model specially designed for underage users, with preconfigured parental protection tools.

The Child SIM allows universal access to parental protection regardless of the family's technological skills, as it places the responsibility for protection under the umbrella of the telecommunications provider.

By default, the Child SIM should include the following functions:

- Content filtering by configuring the APN (Access Point Name) with a DNS (Domain Name Server) service that blocks access to sites and servers offering:
  - Pornography
  - Betting and gambling
  - Drugs
  - Violence
  - Eating disorders, self-harm
  - P2P services
  - Online games
  - Social media
- Enabling search engines' "Safe Search" feature by default.[38]
- Ability to set daily/monthly data traffic limit.
- Protecting windows for screen breaks with the ability to automatically disconnect the terminal from the internet during the night, maintaining access to emergency services (e.g. calling 112, etc.).

[37] D'acord amb el punt 7.4 "Sobre les entitats que podrien portar a terme la verificació d'edat".

- Ability to identify unhealthy usage patterns and suggest connectivity breaks to the user.

The "Child SIM" would have the capacity to become (de facto) an attribute identifying that the user is underage, given that:

- They are provided voluntarily.
- They actively state that they are underage.
- Their issue and validation is supported by a trusted third party (the operator who carries out KYC and line activation).

The "Child SIM" would also have the capacity to become a self-declaration certificate of the "Child User" attribute, available to third parties without the need to share any of the user's other personal data. In this way, a "Child SIM" user would have by default:

- Age-appropriate access to app stores.
- Profiles and parental protection features for social media.
- An unambiguous identifier for online platforms to apply protection, such as:
  - No individualised advertising profiling of the user.[39]
  - Activating child protection systems, safeguarding their privacy and security on the platform.[40]
  - Activating channels for giving warnings, reporting abuse and requesting help, in accordance with the obligations set out in Article 35 of the European Digital Act.

Child Wi-Fi Mode

Internet connectivity operators use hardware elements in the home that are a gateway to the internet, such as the router.

The appropriate firmware (software that manages the hardware) and configuration of the modem/router provide a powerful tool for the digital protection of children.

The CoMB invites operators to offer domestic/family customers the installation of modem/routers with the following functions:

- Home Wi-Fi network segmentation, including the following default segmentations.
  - **General network:** intended for adult residents and iOT devices[41] in the home.
  - **Guest mode network:** intended for guests in the home.
  - **Child mode network:** intended for child residents and guests.
- Enabling the following functions by default in the child mode network:
  - DNS content filtering with pre-activated filters for potentially dangerous content:
    - Pornography
    - Betting and gambling
    - Drugs
    - Violence
    - Eating disorders, self-harm
    - P2P Services
    - Online games
    - Social networks
  - Enabling the "safe search" feature of search engines by default.
  - Ability to set a daily/monthly data traffic limit.
  - Protecting screen break windows with the ability to automatically disconnect devices connected to the Child Mode Network from the internet.
  - Ability to identify unhealthy usage patterns and suggest connectivity breaks to the user.

This technical solution allows operators to universalise parental protection in homes regardless of users' technical skills and allows the family to establish a browsing environment that complements and reinforces educational and communication work among family members.

There are already open source firmware solutions (e.g.: OpenWRT) currently available that incorporate many of the functions suggested in this point, allowing operators to speed up the roll-out of this tool.

Providing DNS services with content filtering

By default, the modems and routers already installed by the operator include a primary DNS and a secondary DNS, although without any content filtering or parental protection capacity.

38 Els principals motors de cerca (per ex.: Google, Bing...) disposen de la funció "safe search" que, en cas d'estar activa, aplica filtres de protecció parental a les consultes fetes per l'usuari.
39 D'acord amb l'Art. 28 punt 2 del Reglament UE 2022/2065 del Parlament Europeu i del Consell del 19 d'octubre de 2022. (Digital Act).
40 D'acord amb l'Art. 28 punt 1 del Reglament UE 2022/2065 del Parlament Europeu i del Consell del 19 d'octubre de 2022. (Digital Act).

41 IOT: Internet Of Things. Dispositius connectats a Internet.

Given the protection capacity offered by an appropriate DNS configuration on all devices connected to the home network, the CoMB invites operators to provide a service that allows the user/customer to activate parental protection via DNS on the modem/router installed at home.

This service would allow families to activate parental protection with minimal (or no) technical action, as the operator could carry out this configuration remotely, without having to send a technician to the home.

Child device configuration service

Given the effectiveness of parental protection tools included in mobile operating systems[42] and the importance of proper device configuration in subsequent use of the terminal (access to the application store, access to potentially dangerous content), the CoMB urges mobile phone operators to include device configuration services aimed at children in their service portfolio.

This initiative aims to universalise access to these tools and to highlight the importance of the proper configuration of devices, especially when they are intended for child users.

3.3. For the developers of online platforms and search engines

Demanding compliance by online platforms and search engines with the obligations established by the Digital Act. Especially for "very large online [platforms] and very large search engines"[43] (those with +45 million users in the EU).

- **NOT showing advertisements presented on the basis of profiling to underage users.**

  This point is of particular strategic interest, as social media are, after all, advertising platforms in which the price of advertising space increases depending on the profile. Eliminating advertising profiling for underage users truncates the platforms' incentive model and reduces the commercial pressure they have on this user segment.[44]

- Establishing the single points of contact required by the Digital Act in relation to:
  - Contact with Member State authorities, the Commission and the European Board for Digital Services.
  - Establishing points of contact for users so they can report incidents (e.g. cyber seduction of children, exposure to potentially dangerous content, etc.).

[42] Temps d'ús per a Apple iOS i Family Link per a dispositius Android.
[43] Art. 33 Digital Act, la llista de les empreses obligades es publicarà i mantindrà actualitzada mitjançant el Diari Oficial de la Unió Europea.
[44] Art. 28 en relació amb la Protecció dels Menors en línia de la Digital Act.

- Giving priority to warnings and complaints from reliable whistleblowers.

  Hence the importance of the public authorities promoting the establishment of Reliable Whistleblowers that allow for the channelling and timely proper attention to user warnings and complaints.

- Responding to the obligation[45] for an annual risk assessment, with special attention to:

  "Any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health ***and children and the serious negative consequences for people's physical and mental well-being****"*.[46]

- Implementing mandatory risk reduction measures, including:
  - Adapting the design, features, and interfaces of applications.
  - Moderating, removing and blocking illegal and potentially harmful content.
  - Adopting specific measures to protect children's rights, including:
    - Age verification tools.
    - Parental control tools.
    - Tools to help children report abuse.
    - Tools to enable children to call for help.

- Undergoing independent audits, with comments, showing whether or not they have met their obligations in relation to codes of conduct, online advertising, and crisis protocols (affecting public health and safety).

- Submitting to data requests, scrutiny of algorithmic systems and content recommendation systems for users passed on by the Digital Services Coordinator.

- Incorporating into their organisations the "Compliance Check" function to ensure internal compliance with the platform's obligations under the Digital Act.[47]

- Applying protective measures against improper use of their services (e.g. dissemination of clearly illegal and potentially dangerous content), including:
  - Notifying users.
  - Suspending access to its services.

- Adapting the design and interface of the application for child users:
  - Establishing protective measures children against content that could harm their physical, mental and moral development.[48]
  - Establishing tools allowing conditional access to potentially dangerous content.
  - Incorporating content moderation tools aimed at detecting, identifying and acting against illegal content.[49]

[45] Aplicable només als serveis de "gran dimensió".
[46] Article 34 apartat "d" de la Digital Act.
[47] Aplicable només als serveis de "gran dimensió".
[48] Punt 89 del preàmbul del Digital Act.
[49] Art Digital Act.

Demanding that developers take responsibility for implementing tools and strategies aimed at protecting children beyond compliance with the regulatory framework:

- Applying the "child by default" principle.
- Allowing users to set self-limiting functions:
  - Time limit alerts.
  - Making it easy for the user to set screen breaks and reminders.
- Establishing different "user statuses" during the provision of a new profile based on age verification:
  - **NOT-allowed user status:**
    - Users who actively declare that their age is below the PEGI code established by the developer.
    - Users included in the self-exclusion register.
    - Users with a Child SIM.
  - **Pending/child user status:**
    - Underage users (regardless of PEGI age rating).
    - All users who have not proven to be of legal age (child by default principle).

    For this user status, invite the developer to set function limits on the application until the user confirms they are of legal age.

    These limitations provide a positive incentive for the user (to confirm their age) and for the developer to refine the user base and adapt function availability to the requirements of the Digital Act. This function limitation may include:
    - Daily usage time limit.
    - Daily limit on interactions within the app.
    - Profile set to "private" mode by default.
    - Limitation of "social recognition" features (e.g. "Like" button) linked to approval-seeking.
- **Active user:**
  - Users who have **actively** confirmed that they are of legal age.

  In this status, the user has access to all functions and can set their profile as public to freely interact with other users of the platform.

3.4. For families

- Caregivers should consider restricting screen use in bedrooms and establishing screen-free periods at home (during meals, homework, and bedtime).
- Not exposing children between the ages of 0-6 to screens.
- From the age of six, when children begin using screens, making sure they are always accompanied by an adult when doing so.
- Avoiding screen use while feeding a baby. Prioritising eye contact and expressiveness with the child.
- Delaying the adoption of the first smartphone until age 16. If the child needs a tool to communicate before that age for emergencies, considering "dumb" devices.[50]
- BEFORE handing over the first smartphone, setting up the home network and devices with parental protection systems aimed at:
  - Filtering accessible content and applications.
  - Managing time windows for device usage.
  - Managing time limits for certain applications.
  - Protecting rest.
- Establishing a "Technology Contract" that establishes limits, use, recognition of the economic value of the device, and the child's obligations when using it. And preventing the device from becoming a "bargaining/punishment chip".
- Including the use of video games within the home (both by minors and by adults when they are in front of minors) in the scope of the family technology contract. Becoming familiar with PEGI coding and being aware that overexposure or early exposure to this type of content can cause pathologies.[51]
- Promoting recreational and social alternatives beyond screens.
- Considering the age of adoption of social networks and before a creates a profile, remembering that:
  - The age of digital consent in Spain is 14 (children under that age require the consent of the holder of parental authority or guardian).
  - The actions of children in the digital environment may have legal (civil and/or criminal) consequences and the scope of this responsibility may affect the holder of parental authority, as well as civil liability towards third parties.

50 Relació d'alternatives a telèfons intel·ligents suggerides per la organització "Wait until 8th" als EUA. https://wwwwaituntil8th.org/devices

51 Afectacions patològiques d'acord amb el registre DSM5 de l'Organització Mundial de la Salut (OMS).

- The age of when this criminal liability begins in Spain is 14.
- The recommendations of international child protection organisations in the field of multimedia content on the age of adoption for social media should be taken into account:
  - Common Sense:[52] from 15 years old.
  - Protect Young Eyes:[53] from 16 years old.

• On mobile devices:
- Installing and enabling parental protection for the device's operating system (Family Link for Android, Screen Time for iOS). Taking special care to:
  - Set usage and screen break windows (do not disturb mode).
  - Set daily app usage limits.
  - Set content filtering for:
    - Web browsing using the device.
    - App acquisition.
    - Access to streaming services (video, music, podcasts, etc.).
  - On iOS devices, activating the following functions is recommended:
    - Communication security:[54] detection and blocking, sending/receiving images and videos inappropriate for children.[55]
    - Screen distance: detection and warning of risks to visual health due to inappropriate distance between the screen and the eyes.
- Avoiding "unlimited data" plans for lines associated with children.
- Requesting the mobile telephone operator to activate parental protection systems at network level on the line assigned to the child intended to manage access windows and filter content:
  - Orange: Kids ready
  - Vodafone: Secure Net
- Including the criterion of "availability of parental protection systems" in their telecommunications provider selection process. Actively requesting and asking the supplier about the availability of these options.
- Recommending the installation of content moderation and social media cyberbullying alert apps, such as:
  - Surfie- Puresight[56]
  - Bodyguard[57]
  - Bark[58]

[52] Common Sin: https://www.commonsense.org/
[53] Protect Young Eyes: https://protectyoungeyes.com/
[54] Requereix iOS 15.2 o superior, iPats 15.2 o superior, watchOS 9 o superior.
[55] Inclou contingut sexual explícit.
[56] Surfie Puresiht - https://www.puresight.com/
[57] Bodygard - https://www.bodyguard.ai/
[58] Bark - https://www.bark.us

• On the home network:
- Demanding that the telecommunications operator provide parental protection systems by default in the company's router (Child Mode Wi-Fi project).
- In the absence of a fibre operator offering Child Mode Wi-Fi:
  - Enabling content filtering via DNS, and setting up the (primary and secondary) DNS on both the router and the child's devices.59
  - Segmenting the home network to establish access exclusively for children's devices.
  - Installing protective firewalls and assigning content filtering rules and usage limits to children's devices.

• Registering and setting up social media, messaging apps, and other sensitive apps:
- Remembering the importance of respecting minimum ages for activating accounts on certain apps on devices.
  - If the family has set up parental protection systems properly, the app store will perform preventive filtering based on the user's age.
- Becoming familiar with and following the recommendations of the PEGI (Pan European Game Information) and IARC (International Age Rating Coalition) ratings before purchasing content (Apps, video games).
- For children:
  - Those below the age of digital consent should NOT install the app.
  - Those who are over the age of digital consent (14 years):
    - ALWAYS, WITHOUT EXCEPTION, giving the child's actual data of birth.
    - Setting the profile to "private/restricted" and/or disabling all features linked to the "public/open" profile.
    - Setting up protection systems (usage limits, content filtering and content moderation).
  - Parents are recommended NOT to install the application if it does not include parental protection/content moderation systems.

• Warning and complaining:
- Exercising the rights granted to users by the Digital Act to activate the warning and complaint systems through any of the enabled channels:
  - Activating the "Point of contact for service recipients " enabled by the app developer for warning of incidents regarding potentially dangerous content and interactions (especially in the case of children).[60]

[59] OpenDNS, solució de la companyia Cisco, ofereix un servei de DNS amb filtrat de continguts gratuit per a usos domèstics.

- Reporting incidents and/or potential non-compliance to:
  - The Digital Services Coordinator assigned by the Member State (EU).
  - Any of the "Trusted Whistleblowers" appointed by the Digital Services Coordinator of the Member State.[61]
  - Any of the "collective representation bodies" authorised to represent users interests in relation to online platforms.[62]

[60] D'acord amb l'Art. 12 del Reglament UE 2022/2065 del Parlament Europeu i del Consell del 19 d'octubre de 2022. (Digital Act).
[61] D'acord amb l'Art. 22 del Reglament UE 2022/2065 del Parlament Europeu i del Consell del 19 d'octubre de 2022. (Digital Act).
[62] D'acord amb l'Art. 86 del Reglament UE 2022/2065 del Parlament Europeu i del Consell del 19 d'octubre de 2022. (Digital Act).

4 Next steps for the CoMB

- The CoMB will set up a committee to update and monitor the degree of compliance with the recommendations/obligations by telecommunications operators and online platforms.
- Calling on civil society and stakeholders (telecommunications operators, online platforms, etc.) to reach a consensus on the risks to public health resulting from premature exposure and overexposure to screens.
- The CoMB will request meetings at the highest level with the aim of passing on its recommendations on protecting public health in front of screens to:
  - Public institutions with regulatory powers (CNMC, AEPD).
  - Public-private institutions (PEGI, IARC, ISFE) responsible for digital content classification systems.
  - The main telecommunications operators and online platforms.
- Promoting, driving and joining in with strategic projects, such as:
  - Child SIM Project
  - Child Mode Wi-Fi Project
  - Screen-Free Spaces Project
  - Age verification systems
- Updating health protocols where there is a health impact resulting from the premature or excessive use of screens to facilitate the actual implementation of the tools enabled in the Digital Act.
- Promoting medical and scientific research on the effects of exposure to screens and certain types of applications on the health of users, especially children.
- Becoming a "collective representation body" as set out in Article 86 of the Digital Act, allowing it to pass on cases and complaints affecting the health of children that have been identified by health professionals to be forwarded to the Digital Services Coordinator
- Actively participating in the development of codes of conduct for search engines, online platforms and other intermediary services, particularly as established in the measures to reduce systemic risks and illegal content (including content potentially harmful to children).[63]

[63] Art. 45 punt 1 i 2 del Reglament UE 2022/2065 del Parlament Europeu i del Consell del 19 d'octubre de 2022. (Digital Act).

- Ensuring that influencers comply with their obligations when promoting products or services when these are potentially dangerous to public health (eating disorders, misinformation about health and unrealistic content related to beauty or appearance, promotion of self-harm, etc.). The CoMB will ensure compliance with the obligation to be included in the state register of providers of audiovisual communication services and compliance with child protection obligations.[64]
- Publicising among healthcare professionals the tools, protocols, best practices, and alternatives to apply in cases where the medical diagnosis shows up an incident associated with screen use.

[64] Art. 94 de Llei 13/2022, de 7 de juliol, General de Comunicació Audiovisual.

5 Appendices

5.1. Appendix I: Bibliography

Manifest Infància i Pantalles: https://sites.google.com/view/manifestinfanciaipantalles/inici

Ús adequat i prevenció de l'addicció a les pantalles en infants i adolescents: https://www.althaia.cat/althaia/ca/usuaris/portal-de-salut-1/grups-de-pacients/documents-adjunts/documents-salut-mental/llibret-us-tic-correccions-2022-web.pdf

Les Tecnologies digitals a la infància, l'adolescència i la joventut: https://govern.cat/govern/docs/2022/09/28/11/29/4930d590-e484-42eb-a98a- a8444f4563a9.pdf

Guia preventiva sobre entorns digitals adreçada a professionals que treballen amb adolescents: https://scientiasalut.gencat.cat/bitstream/handle/11351/6579/guia_preventiva_sobre_en%20torns_digitals_adre%c3%a7ada_professionals_que_treballen_amb_adolescents_2020.%20pdf?sequence=4&isAllowed=y

Exploring adolescents' perspectives on social media and mental health and well-being - A qualitative literature review (Calancie et al., 2017; Kennedy y Lynch, 2016; Singleton et al., 2016; Weinstein, 2018): https://www.researchgate.net/publication/361174035_Exploring_adolescents'_perspectives_on_social_media_and_mental_health_and_well-being_-_A_qualitative_literature_review

La regulació de l'ús dels mòbils als centres educatius (Consell Escolar de Catalunya del 12 de desembre de 2023): https://govern.cat/govern/docs/2023/12/21/13/23/5eb82d8a-d509-431b-9e11-f2fb7f572028.pdf

Social media use and health risk behaviors in young people: systematic review and meta- analysis: https://www.bmj.com/content/383/bmj-2022-073552

Exploring adolescents' perspectives on social media and mental health and well-being - A qualitative literature review, Popat & Tarrant, 2023: https://pubmed.ncbi.nlm.nih.gov/35670473/

Demanda de THE CITY OF NEW YORK, THE CITY SCHOOL DISTRICT OF THE CITY OF NEW YORK; AND NEW YORK CITY HEALTH AND HOSPITAL CORPORATION contra plataformas en línea (Meta, Youtube, TikTok, Snapchat): https://www.nyc.gov/assets/home/downloads/pdf/press-releases/2024/2024-02-14%20City%20of%20New%20York%20Complaint%20021424.pdf

5.2. Appendix II: Definitions and acronyms

AEPD	Agencia Española de Protección de Datos (Spanish Data Protection Agency). **https://www.aepd.es/**
APN	Access Point Name.
CNMC	Comisión Nacional de los Mercados y la Competencia (National Commission on Markets and Competition). **https://www.cnmc.es/**
DNS	Domain Name Server.
IARC	International Age Rating Coalition. **https://www.globalratings.com/**
ISFE	Interactive Software Federation of Europe. **https://www.videogameseurope.eu/**
KYC	Know Your Customer, a set of procedures, tasks and actions intended to establish effective identification of the client-user.
LMS	Learning Management System.
OAuth	Open Authorization is an open standard allowing a simple processes for websites or computer applications.
PIV	Plataforma de intercambio de vídeos.
PEGI	Pan European Game Information. **https://www.pegi.info**
RGIAJ	Registro General de Interdicciones de Acceso al Juego (General Register of Prohibitions on Access to Gambling).
VSP	Video Sharing Platform.

5.3. Appendix III: Regulatory framework

LGCA: Spanish Audiovisual Communication Act 13/2022, of 7 July.

LOPDGDD: Spanish Personal Data Protection and Guaranteed Digital Rights Act 3/2018, of 5 December.

Digital Act: Regulation (EU) No. 2065/2022 of the European Parliament and of the Council of 19 October 2022.

eIDAS: Regulation (EU) No. 910/2014 of the European Parliament and of the

Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

eIDAS-2: Proposal for a regulation amending eIDAS https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0281

LORPM: Spanish Criminal Responsibility of Children Act 5/2000 of 12 January.

5.4. Appendix IV: Members of the Expert Group promoted by the CoMB

Rosa Calvo
Psychiatrist working with children and teenagers. Medical doctor from the University of Barcelona (UB) and assistant lecturer at the UB. Researcher at IDIBAPS and CIBER-SAM. Head of Child and Adolescent Psychiatry and Psychology Service Section at Hospital Clínic, Barcelona. Member of the Governing Board of the Barcelona Medical Association and president of the scientific committee of AEPNYA.

Jordi Camós
Expert in digital business models, tools and trends. Author of *La otra cara de las pantallas* (The Other Side of Screens), a lecture providing an understanding of how games, apps and social networks are designed to condition people's behaviour, their effects and how certain habits can be changed. He also helps companies develop strategic projects and train executives on digital opportunities.

Cesc Gummà
Co-founder of the Anne Private Foundation and its General Director from 2002 to 2023. Extensive experience in business and social care work environments. Promoter of the lecture *La otra cara de las pantallas* and the Members of the Expert Group promoted by the CoMB.

Xavier Ibarz
Member of the Catalan police force's Central Public Service Unit intended to prevent the misuse of the internet and social media by children. Since 2010, he has worked in community relations and has provided more than 1,000 information sessions at schools and colleges in Catalonia.

Marc Masip
Graduate in Psychology from the University of Barcelona and expert in addiction to new technologies. Member of the Governing Board of the Digital Transformation Advisory Council of the Madrid Region. Member of the Governing Board of the Private Schools of Catalonia (EPIC). Author of the book DESCONECT@. Lecturer and populariser.

Lluís Mulero
Technology consultant and cyber activist in publicising tools and strategies for preventing cyber addictions. Promoter of the blog www.habitoscibersaludables.com and author of the book La Superguía de protección digital para tus hijos (The Super Guide to Digital Protection for Your Children).

Silvia Ramón-Cortés
Journalist. Communication consultant and outside lecturer at the UOC on the Corporate Communication master's degree course.

Marc Ferreira
Graduate in Psychology and Anthropology from the University of Barcelona, holder of a master's degree in Cognitive Social Therapy and a DEA (Diploma in Advanced Studies) in Social and Cultural Anthropology from the University of Barcelona. Psychologist and healthcare director at Eatica.

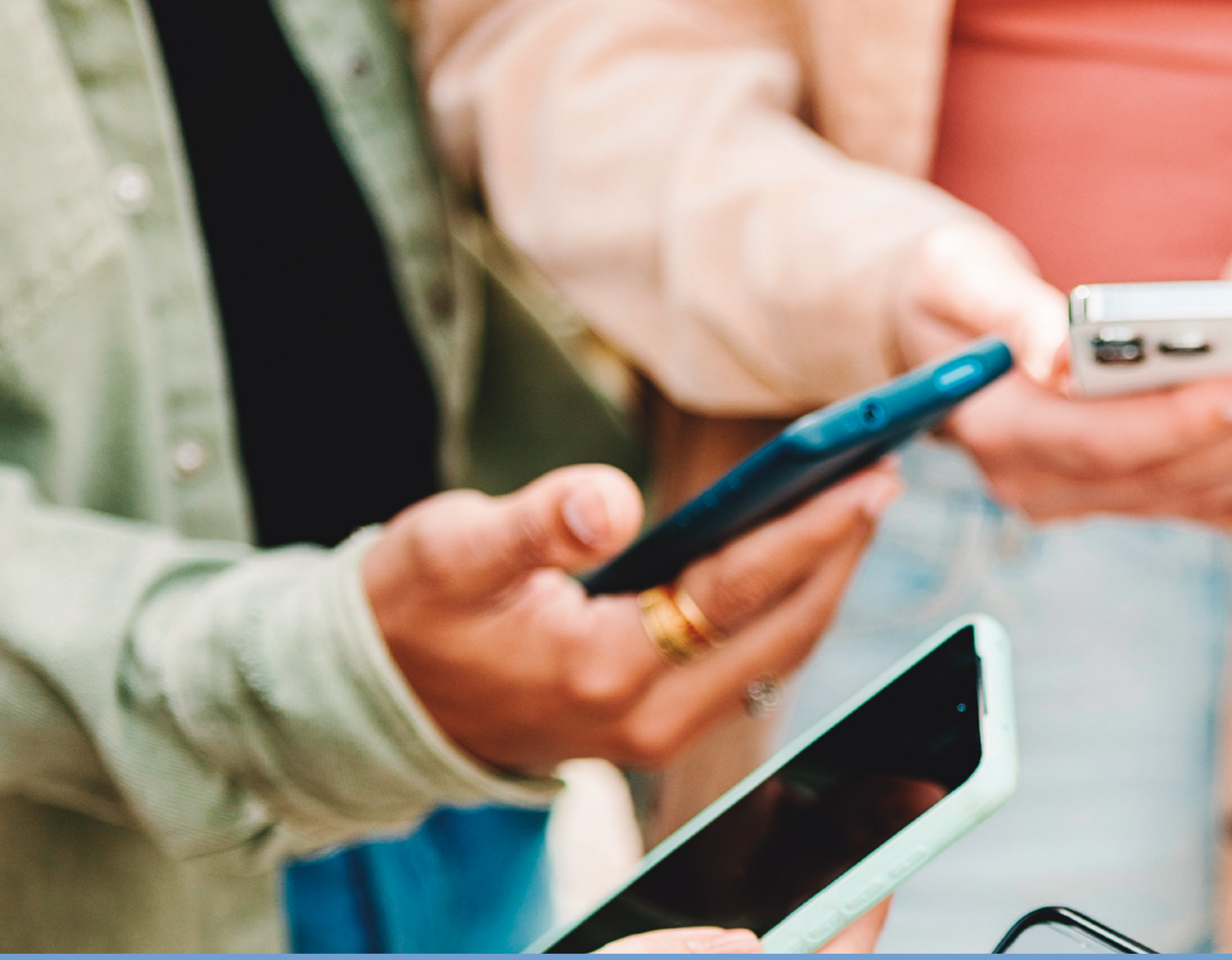
Tomàs Moré
Head of the Culture Unit of the Catalan Cybersecurity Agency's Cybersecurity Innovation and Competence Centre. Member of the team behind the "Safe Internet" campaign.

Montse Sánchez
Founder and director of Eatica.

Jordi Royo
Psychologist. Clinical Director of Amalgama7.

Toni Calvo
Psychologist. Psychotherapist. Director of the CoMB's Social Protection Programme. Director of the Galatea Foundation.

Natàlia Raguer
Social worker. Sociologist. Holder of a master's degree in Social Gerontology. Coordinator of the CoMB Social Protection Programme.



Col·legi de Metges
de Barcelona