PROTECTING CHILDREN IN THE DIGITAL WORLD: FROM GLOBAL EXPERIENCE TO THE TRA'S VISION FOR A NATIONAL FRAMEWORK IN LEBANON

Raising awareness and sharing practical guidance on protecting children in the digital world.

By Dr. Hayssam Serhan, TRA Board Member & Head of Information & Consumer Affairs Unit

For children, the digital environment is an integral part of their everyday life, a space where they learn, communicate, play, create, and connect with others. While digital technologies offer significant opportunities, they also expose young users to risks including harmful content, cyberbullying, manipulation, and exploitation.

Protecting children online begins with parents and families, who play a central role in guiding them, recognizing risks, and creating a safe environment for open communication. However, they cannot carry this responsibility alone. Effective protection requires coordinated action from public institutions, schools, law enforcement agencies, telecommunications providers, technology companies, and civil society.

Building on its longstanding work in this field, the Telecommunications Regulatory Authority is calling for a comprehensive national framework that enables children to benefit from the digital world safely and responsibly.

ONLINE HARM IS REAL, AND IT CAN REACH ANY CHILD

The internet can bring risks directly into a child's home, classroom, or personal device. Harm may come from strangers, other children, misleading content and online communities.

Children and teenagers may encounter:

- **Cyberbullying**, humiliation, threats, and online harassment.
- **Grooming**, manipulation, sexual exploitation, and coercion by online predators.
- **Violent**, extremist, sexually explicit, or otherwise age-inappropriate content.
- **Identity theft**, impersonation, phishing, scams, and fraudulent in-app transactions.
- **Pressure to share** personal photographs, videos, passwords, locations, or private information.
- **Excessive or compulsive use** encouraged by autoplay, notifications, endless scrolling, and other persuasive platform features.
- **Artificial intelligence-generated images**, deepfakes, manipulated content, and false information that can be difficult for young users to recognize.
- **Privacy violations** that may affect a child's safety, dignity, and digital reputation.

The consequences can extend far beyond the screen. Online harm can affect a child's emotional well-being, education, relationships, confidence, privacy, reputation, and, in serious cases, physical safety. International guidance emphasizes that protecting children requires a coordinated approach that reduces risks while preserving their ability to learn, participate, and exercise their rights online.

Traditional advice alone is no longer sufficient, as children navigate increasingly complex digital environments shaped by algorithms, artificial intelligence, online games, social platforms, and private messaging. While parents and schools remain essential, effective protection also requires safer platform design, responsible industry practices, and clear national mechanisms for prevention, reporting, and response, so that children can benefit from technology in a secure, age-appropriate, and accountable environment.

HOW OTHER COUNTRIES ARE RESPONDING

Around the world, governments and regulators are moving from voluntary recommendations toward stronger obligations for digital platforms.

Australia: placing responsibility on platforms.

Australia introduced a minimum age of 16 for accounts on certain social media platforms. The measure entered into effect on 10 December 2025 and requires covered platforms to take reasonable steps to prevent users under 16 from creating or maintaining accounts.

Responsibility for compliance rests with the platforms, not with children or their parents. The Australian approach seeks to reduce children's exposure to harmful content, excessive engagement, cyberbullying, exploitation, and platform features that may negatively affect their health and well-being.

The United Kingdom: mandatory child-risk assessments.

Under the United Kingdom's Online Safety Act, services likely to be accessed by children must assess the risks children may encounter and introduce appropriate protections. Ofcom, the UK communications regulator, oversees the Act implementation and has issued codes and guidance covering children's risk assessments, age assurance, safer service design, and protection from harmful content. The main children's safety duties came into force in July 2025.

The European Union: protection by design.

The European Union's Digital Services Act requires online platforms to take stronger measures to safeguard minors. It includes enhanced protection from age-inappropriate content, greater accountability for major platforms, and a ban on targeted advertising directed at minors. In July 2025, the European Commission also published detailed guidelines on the protection of minors under the Act.

Although these models differ, they reflect a clear international direction: protecting children cannot depend exclusively on parental supervision. Digital platforms and service providers must also assume greater responsibility for the environments they create.

THE TRA'S LEADERSHIP IN CHILD ONLINE PROTECTION

Child Online Protection is not a new area of engagement for the TRA. The Authority has already built valuable experience through regulatory work, awareness initiatives, educational cooperation, regional partnerships, and international participation.

A central TRA achievement has been the creation of e-Aman, a dedicated platform offering parents, educators, and children practical guidance, educational resources, and tools for safer internet use.

The TRA has also:

- Cooperated with the Higher Council for Childhood on national Child Online Protection initiatives.
- Organized and participated in workshops, presentations, and awareness activities with educational institutions and community organizations.
- Worked with the Ministry of Education to support the inclusion of online safety awareness in educational materials and public-school booklets.
- Coordinated with the Ministry of Telecommunications to incorporate child online safety principles into the Code of Ethics for Value Added Services.
- Contributed to the AREGNET Child Online Protection Project and the preparation of a regional Code of Practice for telecommunications service providers, subsequently adopted by AREGNET member regulators.
- Participated in initiatives involving the Internet Society, the Lebanese Internet Governance Forum, schools, and civil society partners, including World Vision Lebanon.

These achievements provide Lebanon with an important foundation on which to build a more structured and sustainable national framework.

A PROPOSED NATIONAL FRAMEWORK FOR LEBANON

Lebanon now needs to move from valuable but fragmented activities toward a coordinated national Child Online Protection framework.

The TRA proposes an approach built around four main interconnected pillars:

PILLAR 1: National coordination and clearly defined responsibilities
A permanent coordination mechanism should bring together the relevant ministries, regulators, law enforcement bodies, judicial authorities, educational institutions, child-protection organizations, telecommunications operators, technology companies, and international partners.

This mechanism would clarify institutional responsibilities, reduce duplication, facilitate referrals, and ensure that initiatives form part of a coherent national strategy.

In this context, the TRA is committed to requiring telecommunications operators and service providers to implement appropriate blocking and filtering mechanisms at the national level, in line with applicable laws and regulations, to help protect children and other vulnerable users online.

PILLAR 2: Awareness and digital literacy
Children must be educated on how to recognize manipulation, protect their privacy, verify information, respond to cyberbullying, report suspicious behavior, and seek help.

Parents and educators also need practical, accessible guidance that reflects the applications, platforms, games, and technologies children are actually using. Awareness should not be limited to occasional campaigns; it should be embedded in school programs, family discussions, teacher training, and community initiatives.

PILLAR 3: Safer and more responsible digital services

Telecommunications providers and digital platforms should be encouraged, and where appropriate, to adopt child-sensitive practices, accessible parental controls, strong privacy settings, effective age-assurance measures, clear reporting tools, and safer default settings for younger users.

Industry codes and regulatory guidance can help establish common expectations and promote safety by design.

PILLAR 4: Research, evaluation, and international cooperation

Lebanon needs reliable information about the online experiences of children, the risks they encounter, and the effectiveness of existing protective measures.

Regular research and consultation would allow policies to evolve alongside technology. International and regional cooperation would also enable Lebanon to benefit from emerging standards, technical expertise, and successful regulatory practices.

WHAT PARENTS AND CAREGIVERS CAN DO TODAY

Legislation and national coordination are essential, but protection also begins with everyday communication at home.

Parents and caregivers should:

- **Speak regularly with children** about what they watch, play, share, and experience online.
- **Create an atmosphere in which children can report uncomfortable situations** without fear of punishment or losing access to their devices.
- Review account privacy settings, location sharing, application permissions, contact lists, and parental-control options.

- **Agree on age-appropriate rules** concerning screen time, online purchases, unknown contacts, livestreaming, and the sharing of photographs or personal information.
- **Teach children a simple response to harmful behavior**: stop, block, report, save the evidence, and tell a trusted adult.
- **Remind children that people online may not be who they claim to be.**
- **Explain that photographs, messages, and personal details can be copied or redistributed**, even when shared privately.
- **Seek immediate assistance** when a child faces threats, grooming, exploitation, blackmail, or pressure to share intimate content.

Technical controls help, but they can't replace trust and open communication. The goal isn't surveillance — it's making sure children feel safe asking for help before a problem becomes a crisis. This is a balance that international guidance recommends as well.

A SHARED RESPONSIBILITY AND A NATIONAL PRIORITY

Child Online Protection is a national priority for the TRA. The Authority is committed to strengthening online safety through awareness initiatives, capacity building, stakeholder engagement, and coordinated action with government institutions, civil society organizations, educational institutions, and other relevant stakeholders.

Going forward, the TRA will continue to promote practical measures that empower children, support parents and educators, and reinforce Lebanon's national response to online risks, helping build a safer and more responsible digital environment for children.

Protecting children online is a shared responsibility. Parents, children, teachers, caregivers, and community members are all encouraged to seek guidance or report any concern related to a child's online safety and well-being.

For information, support, or assistance, please visit our dedicated website at https://e-aman.tra.gov.lb or contact us at info@tra.gov.lb.