Protecting Children

in the Digital Environment

Social Media Restrictions, Platform Accountability, and Human Rights Implications for Lebanon

الجمهورية اللبنانية
الهيئة الوطنية لحقوق الانسان
المتضمنة لجنة الوقاية من التعذيب
National Human Rights Commission
including the committee for the prevention of torture

Title: Protecting Children in the Digital Environment | Social Media Restrictions, Platform Accountability, and Human Rights Implications for Lebanon

Publisher: The Lebanese Republic | The National Human Rights Commission, which includs the Committee for the Prevention of Torture (NHRC-CPT)

Author: Bassam Alkantar | Commissioner for International Relations and Information at NHRC-CPT.

First Edition: 2026

📍 **Address:** Serhal Building, First Floor, Sami El Solh Boulevard, Beirut, Lebanon.

📧 **Email:** info@nhrclb.org

🌐**Website:** https://nhrclb.org

☎️**Hotline:** +961 3 923 456

Facebook: http://fb.nhrclb.org

X: http://twitter.nhrclb.org

Instagram: http://insta.nhrclb.org

YouTube: http://yt.nhrclb.org

Flickr: https://www.flickr.com/photos/145354751@N08/

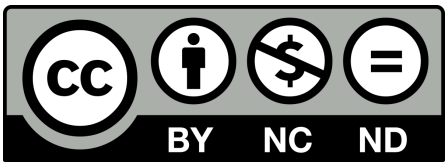
Bluesky: https://bsky.app/profile/nhrclb.bsky.social

Tumblr: https://www.tumblr.com/nhrclb

Mastodon: https://mastodon.social/@nhrclb

LinkedIn: https://www.linkedin.com/company/nhrclb/

Threads: https://www.threads.com/@nhrc_lb



The views expressed in this report are those of the National Human Rights Commission, including the Committee for the Prevention of Torture, and do not necessarily reflect the views of any parties mentioned in the report or of any past or current partners.

The National Human Rights Commission, which includes the Committee for the Prevention of Torture, works to protect and promote human rights in Lebanon in accordance with the standards set out in the Constitution, the Universal Declaration of Human Rights, relevant international treaties and conventions, and domestic laws aligned with these standards. It is an independent national institution established under Law No. 62/2016, pursuant to the United Nations General Assembly resolution (Paris Principles) which governs the creation and functioning of national human rights institutions. The Commission also serves as the National Preventive Mechanism against torture, in line with the provisions of the Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, which Lebanon acceded to under Law No. 12/2008.2008.

1. Executive Summary

Digital technologies have become an integral part of the lives of children and adolescents in Lebanon and around the world. Social media platforms now function as key spaces for communication, education, identity formation, entertainment, and civic participation. At the same time, these technologies expose children to serious risks, including cyberbullying, online harassment, harmful content, exploitative data practices, addictive design features, online grooming, and emerging harms linked to artificial intelligence. These developments have prompted governments to adopt or consider new forms of regulation. Yet the central legal and policy challenge remains how to protect children effectively without undermining their rights to freedom of expression, access to information, privacy, education, and participation.

This report, issued by the National Human Rights Commission, which includes the Committee for the Prevention of Torture, examines this challenge from a human rights perspective, with a particular focus on Lebanon. It analyzes international regulatory trends, the relevant international legal framework, recent Lebanese legislative and policy developments, and the growing importance of cybercrime regulation and artificial intelligence governance. It concludes that while the protection of children in the digital environment is a legitimate and pressing objective, restrictive approaches based primarily on blanket access bans are unlikely to provide a complete or sustainable solution. A more effective approach requires a comprehensive and rights-based framework combining child protection, platform accountability, data protection, cybercrime cooperation, transparency, and regulation of artificial intelligence.

The report first situates Lebanon within a broader international policy debate. In Australia, legislation adopted in December 2025 requires social media companies to prevent individuals under sixteen from opening or maintaining accounts. In Malaysia, similar restrictions have been proposed under the Online Safety Act 2025, potentially through digital identity verification systems. By contrast, the European Union has largely favored platform accountability measures through instruments such as the Digital Services Act and the General Data Protection Regulation, which impose obligations on technology companies to mitigate systemic risks, protect user data, and restrict targeted advertising to minors. These comparative examples show that states are pursuing divergent regulatory paths, some centered on access restrictions, others on the regulation of platform business models and digital ecosystems.

The report highlights the concerns raised by civil society organizations and human rights defenders, including Amnesty International, regarding age-based bans on children's access to social media. Such restrictions may be circumvented in practice, including through false age declarations or alternative accounts, which may push children into less visible and potentially less safe digital spaces. Measures relying on biometric data, facial recognition, or document-based age verification may also create significant risks to privacy and data protection. More fundamentally, access restrictions may interfere with children's rights to receive and impart information, engage in public debate, and participate in social and

cultural life. The report therefore stresses that effective protection cannot be limited to restricting access, but must address the design, operation, and accountability of digital platforms themselves.

International human rights law provides the governing framework for assessing these issues. Lebanon is bound by the Convention on the Rights of the Child and the International Covenant on Civil and Political Rights. Under these instruments, children are rights-holders entitled not only to protection from harm, but also to privacy, participation, freedom of expression, and access to information. General Comment No. 25 of the UN Committee on the Rights of the Child makes clear that states must ensure children can safely benefit from digital technologies while also protecting them from abuse and exploitation. Regulatory measures must therefore satisfy the principles of legality, necessity, proportionality, and respect for the evolving capacities of the child.

A key finding of the report is that many digital harms affecting children arise not solely from children's presence online, but from the structure and incentives of the digital environment itself. Social media platforms rely heavily on algorithmic recommendation systems, surveillance-based advertising, extensive profiling, and interface designs intended to maximize engagement and prolong attention. These features can amplify harmful, sensational, or misleading content and expose children to patterns of dependency, manipulation, or exploitation. As a result, policies that focus exclusively on restricting children's access risk overlooking the deeper structural drivers of harm. The report therefore supports regulation that includes safety-by-design, stronger protections for children's personal data, algorithmic transparency, and corporate accountability.

Within Lebanon, the report identifies important but still incomplete efforts to respond to these challenges. On 26 February 2026, the Council of Ministers adopted Decision No. 13, creating an inter-ministerial committee tasked with preparing a national strategy to regulate and guide children's use of the internet and digital applications. This initiative acknowledges that existing Lebanese laws, including the Penal Code, Law No. 422/2002, Law No. 293/2014, and Law No. 81/2018 on Electronic Transactions and Personal Data, provide only partial protection in the digital sphere and do not amount to a comprehensive framework. The inclusion of the President of the National Human Rights Commission in this committee is a significant step, as it opens the possibility for independent human rights oversight in the development of digital policy.

The report also examines the draft law submitted on 5 February 2026 by MP Tony Frangieh, which would prohibit children under fourteen from using social media platforms and require providers to implement age verification measures. The proposal also includes safeguards relating to children's data and sanctions for non-compliant platforms. While the draft law is motivated by genuine concerns regarding cyberbullying, harmful content, exploitation, and mental health, the report finds that it raises serious human rights questions. These include whether a complete prohibition is proportionate, whether less

restrictive alternatives have been sufficiently explored, and whether the proposed age assurance systems can be implemented in a genuinely privacy-respecting manner. The report concludes that the draft law should not be assessed in isolation, but within a broader framework that also addresses platform design, education, prevention, remedy, and accountability.

The role of the NHRC-CPT is central throughout this process. In line with General Comment No. 25, national human rights institutions have an important function in monitoring children's rights in the digital environment, assessing proposed legislation, raising awareness, and promoting compliance with international standards. For Lebanon, this means that the NHRC-CPT should be recognized not only as a participant in institutional consultations, but as an independent actor capable of reviewing draft laws, documenting harms, receiving complaints, and advocating for a child-sensitive and rights-based digital governance framework.

The report further argues that digital safety for children cannot be achieved without a stronger legal framework for cybercrime and digital evidence. The transnational nature of online harms means that exploitation, harassment, cyberstalking, online grooming, and the dissemination of harmful content frequently involve actors, evidence, and infrastructures located across borders. In this context, the adoption by the UN General Assembly of the United Nations Convention against Cybercrime on 24 December 2024 represents an important development. The Convention establishes a global legal framework for harmonizing cybercrime offences, facilitating digital investigations, and enabling cross-border cooperation in obtaining electronic evidence, while requiring respect for privacy, freedom of expression, and due process.

Lebanon has not yet acceded to this Convention. The report finds that accession would strengthen Lebanon's capacity to investigate and prosecute cybercrime, especially in cases involving children and cross-border digital infrastructures. It would also help modernize national law in relation to digital evidence, mutual legal assistance, and procedural safeguards. At present, Law No. 81/2018 remains Lebanon's principal digital law, but it does not offer a sufficiently comprehensive framework for cybercrime cooperation, modern data protection oversight, or digital justice in line with recent international standards. The report therefore recommends that cybercrime regulation be integrated into child protection policy rather than treated as a separate field.

An additional dimension addressed in the report is the protection of women and girls from technology-facilitated violence. The draft law on the protection of women from digital violence, submitted to Parliament on 25 February 2026, represents a significant legislative initiative to criminalize cyberstalking, online harassment, identity theft, electronic extortion, and the non-consensual dissemination of intimate images. Although primarily focused on women, many of its provisions also have relevance for children and adolescents, especially girls, who face similar forms of abuse in digital spaces.

The report therefore considers this initiative an important part of the broader effort to create a safer and more accountable digital environment in Lebanon.

The report also addresses the emerging challenge of artificial intelligence regulation. Lebanon has recently begun considering several legislative and institutional initiatives in this field. One proposal introduced in 2026 seeks to criminalize the creation, modification, or use of intimate or indecent images and videos generated or altered by artificial intelligence without consent. This draft law responds to the growing threat posed by deepfakes and synthetic media, which can inflict serious reputational, psychological, and social harm, especially on women, children, and other vulnerable groups. The report welcomes this development while emphasizing the importance of legal clarity, proportionality, and safeguards against misuse.

At the institutional level, two separate governance models have been proposed. The first is the draft law establishing the Ministry of Information Technology and Artificial Intelligence, approved by the Council of Ministers in September 2025, which would centralize responsibility for national digital transformation, cybersecurity, personal data protection, and AI policy. The second is the draft law submitted on 4 June 2025 to create a National Artificial Intelligence Authority as an independent body responsible for preparing the national AI strategy, proposing regulatory frameworks, monitoring implementation, and supervising the ethical use of artificial intelligence. These proposals reflect growing recognition that artificial intelligence requires dedicated governance. However, the report finds that the current institutional landscape remains fragmented and lacks a single coherent, rights-based architecture.

Civil society concerns reinforce this assessment. Organizations such as SMEX have raised important questions regarding digital sovereignty, transparency, public-private technology partnerships, and the risks of over-reliance on foreign technology providers. Concerns surrounding the Oracle training agreement announced in December 2025, the incomplete implementation of Law No. 81/2018, and the absence of strong independent oversight mechanisms all illustrate the vulnerabilities of Lebanon's current digital governance framework. Without stronger safeguards, there is a risk that digital transformation may proceed faster than the legal and institutional protections needed to preserve privacy, accountability, and public trust.

Against this background, the report concludes that Lebanon is at a decisive regulatory moment. The country has begun to recognize the need to protect children online, strengthen cybercrime responses, address digital violence, and regulate artificial intelligence. However, current measures remain dispersed across multiple draft laws, ministerial initiatives, and policy proposals that have not yet been consolidated into a coherent framework. The report therefore calls for a comprehensive national strategy that brings together children's rights, data protection, cybercrime regulation, platform accountability, digital literacy, AI governance, and institutional oversight under a single human rights-based vision.

Finally, the report sets out recommendations and expected outcomes directed to the Lebanese Government, Parliament, ministries and public authorities, civil society organizations, and UN agencies and treaty bodies. These recommendations aim to support the development of a coordinated framework that protects children and other vulnerable groups, strengthens accountability for digital platforms and AI systems, improves transparency in digital governance, and aligns Lebanon's laws and institutions with international human rights standards. At the center of this framework, the report places the NHRC-CPT as an independent institution with a critical role in monitoring, advocacy, oversight, and public guidance.

The report's central message is that children should not be treated merely as passive subjects of protection in the digital age. They are rights-holders entitled to safety, dignity, privacy, participation, freedom of expression, and access to information. Protecting them requires not only restrictions where justified, but also education, accountability, transparency, remedy, and institutional reform. A sustainable digital governance framework for Lebanon must therefore place human rights, democratic oversight, and the best interests of the child at its core.

2. Introduction

Digital technologies have become deeply embedded in the everyday lives of children and adolescents. Social media platforms, messaging applications, video-sharing services, online gaming environments, and emerging artificial intelligence tools now shape how young people communicate, learn, access information, express themselves, and participate in social and political life. For many children, the digital environment is no longer separate from offline reality, but an essential extension of it. It offers significant opportunities for education, creativity, community-building, and civic engagement. At the same time, it exposes children to growing risks, including cyberbullying, harassment, harmful content, exploitation of personal data, online grooming, non-consensual image-sharing, addictive design practices, and new forms of manipulation enabled by algorithmic systems and synthetic media.

These developments have generated increasing concern among governments, parents, educators, civil society organizations, and international human rights bodies. In response, a number of states have begun to explore legal and policy measures aimed at regulating children's access to digital platforms, especially social media. Yet such measures raise complex legal and ethical questions. Efforts to protect children online must not come at the expense of their rights to freedom of expression, privacy, access to information, education, and participation. International human rights law requires that any restrictions be lawful, necessary, proportionate, and consistent with the evolving capacities and best interests of the child.

In Lebanon, these debates have become increasingly urgent. Recent legislative proposals, policy initiatives, and institutional discussions reflect growing recognition that the country lacks a coherent framework for governing children's digital lives, cybercrime, digital violence, and the use of artificial intelligence. This report examines these developments through a human rights lens. It argues that protecting children in the digital environment requires more than restrictive access measures. It requires a comprehensive, rights-based framework that addresses platform accountability, data protection, cybercrime cooperation, digital literacy, online gender-based violence, and the governance of artificial intelligence in a manner consistent with Lebanon's domestic and international legal obligations.

3. Global Policy Responses to Children's Social Media Use

3.1. Australia

In December 2025, Australia adopted legislation requiring social media companies to prevent individuals under sixteen from opening or maintaining social media accounts. The law obliges platforms to implement age verification mechanisms and remove existing accounts belonging to minors.[1]

The Australian government justified the legislation as a measure intended to protect children from harmful online content, excessive screen time, and the psychological risks associated with prolonged exposure to social media.

However, the legislation has generated significant debate among policymakers and civil society organizations. Survey data suggests that although a majority of Australians support the intention behind the ban, many believe that children will find ways to circumvent the restrictions and that enforcement may prove difficult.[2]

3.2. Malaysia

In Malaysia, authorities have proposed similar restrictions under the Online Safety Act 2025, potentially requiring digital identity verification mechanisms for online users. Civil society groups have raised concerns that such measures could introduce significant risks to privacy and freedom of expression.[3]

3.3. European Union

Within the European Union, policymakers have generally favored regulatory approaches focusing on platform accountability rather than direct bans on children's access to social media. Instruments such as the Digital Services Act and the General Data Protection Regulation impose obligations on technology companies to mitigate systemic risks, protect user data, and limit targeted advertising directed at minors. [4]

---

[1] Australian Government, Social Media Age Restrictions Legislation, December 2025.
[2] Pureprofile Research Survey on Public Attitudes Toward Social Media Restrictions, 2025.
[3] Amnesty International Malaysia, "Malaysia: Effectively regulate social media to protect children and young people instead of imposing a blanket ban," 3 December 2025.
[4] European Union, Digital Services Act (Regulation EU 2022/2065).

4. Human Rights Concerns Raised by Civil Society

The rapid expansion of digital technologies and social media platforms has generated an equally rapid increase in public debate regarding their impact on children's well-being, development, and rights. Governments across the world have increasingly explored legislative measures aimed at restricting children's access to social media platforms or imposing obligations on technology companies to mitigate digital harms. While many of these initiatives are motivated by legitimate concerns regarding children's safety online, civil society organizations, digital rights advocates, child protection experts, and human rights institutions have raised important concerns regarding the potential unintended consequences of such measures.

These concerns do not challenge the objective of protecting children in digital environments. Rather, they emphasize that regulatory responses must remain consistent with international human rights standards and must address the root causes of digital harm rather than focusing solely on restricting children's access to technology. Civil society organizations have therefore called for balanced regulatory approaches that combine child protection measures with safeguards for freedom of expression, privacy, access to information, and participation in digital spaces.

4.1. Concerns regarding blanket restrictions on children's access to social media

One of the most widely debated policy responses to concerns about children's online safety has been the proposal to prohibit or restrict children's access to social media platforms below a certain age. Proposals of this kind have emerged in several jurisdictions, including Australia, the United Kingdom, and a number of other countries considering legislation addressing children's online safety.

Civil society organizations have raised concerns that blanket prohibitions on children's access to social media may prove ineffective in practice. Research on digital behavior indicates that children and adolescents often possess significant digital literacy and technical adaptability. As a result, they may easily circumvent age-based restrictions by providing false age information, using alternative accounts, accessing platforms through shared devices, or migrating to less regulated digital spaces.

Such outcomes may undermine the intended protective purpose of the restrictions. Rather than reducing children's exposure to harmful online environments, restrictive policies may push children toward platforms that operate with fewer safeguards, weaker moderation systems, or less oversight.

In some cases, children may also seek access to online communities that are more difficult for parents, educators, or authorities to monitor, thereby potentially increasing exposure to risk.

Civil society groups have therefore emphasized that policies focusing exclusively on restricting children's access to platforms may not effectively address the underlying causes of digital harm. Instead, they argue that regulation should focus on the design, operation, and accountability of digital platforms themselves.

4.2. Privacy risks associated with age verification mechanisms

Another major concern raised by civil society organizations relates to the age verification mechanisms that are often required to enforce restrictions on children's access to social media. In many legislative proposals, digital platforms are required to verify users' age in order to determine whether individuals are eligible to create or maintain accounts.

Age verification systems may involve several technological approaches. These include requiring users to upload government-issued identity documents, relying on facial recognition or biometric verification technologies, using artificial intelligence to estimate age based on facial images, or linking online accounts to digital identity systems. While such systems may help enforce age-based restrictions, they may also introduce new risks related to privacy and data protection.

Human rights organizations and digital rights groups have warned that many age verification systems require the collection and processing of highly sensitive personal data. These may include biometric identifiers, facial images, identity documents, or other personal information that can be used to verify identity. If such data is stored, processed, or shared by private companies without adequate safeguards, it may expose children and their families to significant privacy risks.

The potential for data breaches, unauthorized data sharing, profiling, or misuse of personal information has raised concerns among civil society actors. In addition, the use of biometric technologies for age verification may contribute to the normalization of large-scale digital identity verification systems that could have broader implications for privacy and freedom of expression online.

Civil society organizations therefore emphasize that any age verification systems introduced to protect children must adhere to strict principles of data minimization, purpose limitation, and privacy by design. They must also be subject to independent oversight and transparent regulatory safeguards to ensure that children's personal data is not exploited or exposed to misuse.

4.3. Risks to freedom of expression and access to information

Civil society organizations have also emphasized that restrictions on children's access to digital platforms may have implications for their rights to freedom of expression and access to information. These rights are protected under international human rights instruments, including the Convention on the Rights of the Child and the International Covenant on Civil and Political Rights.

In the contemporary digital environment, social media platforms serve as major channels through which individuals exchange ideas, access news and educational resources, and participate in public debate. Young people frequently rely on these platforms to access information about social issues, educational opportunities, and community initiatives. They also use digital platforms to express opinions, share experiences, and participate in discussions affecting their communities.

Civil society organizations therefore caution that overly restrictive measures may limit children's ability to engage with information and public discourse. While protection from harmful content remains a legitimate concern, regulatory approaches must ensure that children retain meaningful opportunities to exercise their rights to communication, participation, and expression.

These concerns are particularly relevant in societies where traditional media environments may not fully reflect the diversity of youth perspectives or where digital platforms provide important spaces for civic engagement and community-building. Limiting children's access to digital spaces without providing alternative channels for participation may inadvertently silence their voices in public debate.

4.4. Structural drivers of digital harm

In recent years, civil society organizations and academic researchers have increasingly emphasized that many harms experienced by children online arise from the structural design of digital platforms rather than simply from children's presence online. Social media platforms are typically built around business models that rely on maximizing user engagement and collecting large volumes of personal data.

Algorithmic recommendation systems are central to these models. These systems analyze user behavior in order to recommend content that is most likely to attract attention and encourage continued engagement. While such systems may enhance user experience, they may also amplify sensational, emotionally provocative, or controversial content because such material often generates higher engagement.

For children and adolescents, this dynamic may result in prolonged exposure to harmful or misleading content. Recommendation algorithms may also reinforce echo chambers or expose young users to material that may negatively affect their psychological well-being.

In addition to algorithmic amplification, the data-driven advertising models used by many social media platforms rely heavily on the collection and profiling of user data. These systems track user behavior across platforms, build detailed profiles of individual users, and use these profiles to deliver targeted advertising.

Civil society organizations have raised concerns that such practices may be particularly problematic when applied to children. Young users may not fully understand the implications of data collection or targeted advertising practices. As a result, children may be exposed to manipulative commercial messaging or behavioral targeting that exploits their vulnerabilities.

From this perspective, civil society organizations argue that regulatory responses should focus not only on children's access to platforms but also on the broader structural features of digital ecosystems. Measures such as restrictions on targeted advertising to minors, transparency requirements for algorithmic systems, and obligations for platforms to conduct risk assessments may therefore play a critical role in protecting children online.

4.5. Digital literacy and empowerment

Civil society actors also emphasize the importance of education and digital literacy in protecting children from online harm. Rather than relying exclusively on restrictive regulatory measures, many organizations advocate for strategies that empower children, parents, and educators to navigate digital environments safely and responsibly.

Digital literacy initiatives may include educational programs addressing online safety, privacy protection, responsible communication, and critical evaluation of digital content. These initiatives can help children develop the skills necessary to recognize harmful content, avoid online exploitation, and respond appropriately to cyberbullying or harassment.

Parents and educators also play an important role in guiding children's digital experiences. Civil society organizations therefore encourage the development of support resources and awareness programs that assist families in understanding digital technologies and promoting healthy digital habits.

Such initiatives recognize that children are not merely passive recipients of digital content but active participants in digital environments. Empowering children to understand and navigate these environments may therefore provide more sustainable protection than restrictive measures alone.

4.6. Toward a balanced regulatory approach

The concerns raised by civil society organizations do not imply opposition to the regulation of digital platforms or the adoption of policies aimed at protecting children online. On the contrary, many organizations strongly support the development of comprehensive regulatory frameworks addressing digital harms.

However, civil society actors consistently emphasize that effective regulation must balance protective objectives with respect for human rights. Regulatory frameworks should therefore include measures addressing platform accountability, data protection, algorithmic transparency, and corporate responsibility while preserving children's rights to expression, information, and participation.

Such an approach recognizes that digital technologies present both opportunities and risks for children. Protecting children in the digital age therefore requires policies that combine safeguards against harm with measures enabling children to benefit from digital innovation in safe and empowering ways.

In this context, the role of human rights institutions, policymakers, educators, civil society organizations, and technology companies becomes essential. Only through coordinated efforts among these actors can regulatory frameworks be developed that effectively protect children while upholding the fundamental rights and freedoms that underpin democratic societies.

5. International Human Rights Framework

5.1. Convention on the Rights of the Child

Lebanon ratified the Convention on the Rights of the Child in 1991. The Convention establishes several rights relevant to children's participation in digital environments.

Article 13 guarantees children the right to freedom of expression, including the freedom to seek, receive, and impart information through any media.

Article 17 recognizes the importance of ensuring children's access to information that contributes to their development.

Article 16 protects children's right to privacy.

States are required to ensure that protective measures adopted in the digital environment respect the principle of proportionality and the evolving capacities of the child. [5]

5.2. International Covenant on Civil and Political Rights

Lebanon is also a party to the International Covenant on Civil and Political Rights. Article 19 protects freedom of expression and access to information.

Restrictions on these rights must satisfy the criteria of legality, necessity, and proportionality under international law. [6]

5.3. UN Committee on the Rights of the Child

In General Comment No. 25 on children's rights in the digital environment, the Committee emphasized that states must ensure children can safely benefit from digital technologies while protecting them from online harms.[7]

---

[5] Convention on the Rights of the Child, Articles 13, 16, and 17.

[6] International Covenant on Civil and Political Rights, Article 19.

[7] UN Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment.

6. Structural Drivers of Digital Harm

Growing research in the fields of digital governance, technology policy, and human rights demonstrates that many online harms experienced by children and adolescents do not arise solely from their presence on digital platforms. Instead, these harms are often deeply connected to the underlying economic incentives, technological architecture, and design features of the platforms themselves. Social media companies operate within business models that prioritize the capture of user attention, the collection of personal data, and the monetization of behavioral information through targeted advertising systems. These structural characteristics shape how information circulates online and how users, including children, interact with digital environments.

Amnesty International's report *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (2019) provides a critical analysis of these dynamics. The report argues that the dominant business model of major technology platforms relies on what has been described as "surveillance capitalism," a system in which companies systematically collect, analyze, and monetize vast quantities of personal data in order to predict and influence user behavior. This model incentivizes platform designs that maximize user engagement and data extraction rather than prioritizing user well-being, safety, or the protection of fundamental rights. [8]

Within this framework, several structural drivers of digital harm can be identified. These include algorithmic recommendation systems designed to maximize engagement, surveillance-based advertising models relying on extensive personal data collection and profiling, and interface design mechanisms engineered to prolong user attention and encourage repeated interaction. Together, these systems create digital environments in which children may be exposed to amplified risks, including harmful content, misinformation, online harassment, and patterns of excessive or compulsive digital use.

6.1. Algorithmic recommendation systems and the amplification of harmful content

One of the most influential structural features of contemporary social media platforms is the use of algorithmic recommendation systems. These systems determine which content appears in users' feeds, which videos are suggested next, and which posts are most prominently displayed. Rather than presenting information chronologically or randomly, platforms rely on complex algorithms that

[8] Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," 2019.

analyze user behavior in order to predict which content is most likely to capture attention and encourage continued engagement.

These algorithms rely on a wide range of behavioral signals, including the amount of time users spend viewing certain content, the posts they like or share, the accounts they follow, and their patterns of interaction with other users. By analyzing these signals, algorithmic systems attempt to identify content that is likely to generate strong emotional reactions or prolonged attention.

While such systems can enhance user experience by recommending content that aligns with user interests, they also create powerful incentives for the amplification of sensational or emotionally charged material. Research indicates that content provoking anger, outrage, fear, or controversy often generates higher levels of engagement. As a result, algorithmic recommendation systems may disproportionately promote content that is polarizing, misleading, or harmful.

For children and adolescents, the implications of this dynamic can be significant. Young users may encounter content that promotes unrealistic body standards, self-harm behaviors, harmful challenges, disinformation, or extreme viewpoints. Once users interact with such content, algorithms may continue recommending similar material, reinforcing exposure through a process often described as algorithmic “rabbit holes.”

Amnesty International and other human rights organizations have argued that these algorithmic amplification mechanisms are not accidental but are closely tied to the economic incentives of the platform business model. Since advertising revenue is directly linked to the amount of time users spend on platforms, companies have strong incentives to design systems that maximize engagement even when such engagement may expose users to harmful content.

6.2. Surveillance-based advertising and data extraction

Another key structural driver of digital harm is the surveillance-based advertising model that underpins the business strategies of many major technology platforms. Under this model, companies collect extensive information about users’ online behavior, interests, relationships, and preferences. This information is then used to construct detailed behavioral profiles that enable highly targeted advertising.

Amnesty International’s analysis describes this system as one in which users are continuously monitored across digital environments. Data may be collected not only from activity on a single platform but also from interactions across multiple websites and applications. Through tracking

technologies such as cookies, device identifiers, and embedded software development kits, platforms can build detailed records of users' browsing habits, search queries, location data, and interactions with online content.

For children, such data collection raises serious concerns regarding privacy and autonomy. Young users may not fully understand how their data is collected or how it is used for commercial purposes. They may also be particularly vulnerable to targeted advertising practices that exploit emotional or developmental vulnerabilities.

Targeted advertising systems may promote products, services, or content that aligns with the behavioral profiles generated by data analysis. For example, users who interact with certain types of content may receive advertisements related to dieting products, cosmetic procedures, or other potentially harmful messaging. In some cases, such advertisements may reinforce harmful stereotypes or encourage behaviors that negatively affect children's well-being.

The surveillance-based advertising model also creates incentives for platforms to collect as much personal data as possible. The more data a company gathers, the more accurately it can predict user behavior and deliver targeted advertisements. As Amnesty International argues, this dynamic can create systemic pressures to expand data collection practices, often in ways that undermine privacy rights and limit individuals' control over their personal information.

6.3. Interface design and attention capture

In addition to algorithmic recommendation systems and surveillance-based advertising models, many social media platforms employ interface design strategies aimed at maximizing user engagement. These design features are often informed by behavioral psychology and are specifically intended to encourage users to remain on platforms for extended periods of time.

Examples of such features include infinite scrolling mechanisms, autoplay functions for video content, push notifications that alert users to new interactions, and visual indicators such as "likes" or engagement counters that reinforce social validation. These design elements can create feedback loops that encourage repeated interaction and prolonged use.

For children and adolescents, these design mechanisms may contribute to patterns of excessive screen time or compulsive engagement with digital platforms. Young users may experience pressure to remain constantly connected in order to maintain social relationships, respond to messages, or monitor online interactions.

Psychological research suggests that features such as intermittent rewards and social validation cues can activate behavioral responses similar to those observed in gambling environments. Notifications, likes, and comments provide small bursts of social feedback that encourage users to check platforms repeatedly.

Amnesty International and other organizations have argued that such design practices raise ethical questions when applied to young users. If platforms are intentionally designed to capture and retain attention, children may find it difficult to disengage from digital environments even when prolonged use negatively affects sleep patterns, academic performance, or mental health.

6.4. Exposure to misinformation and harmful narratives

Another consequence of engagement-driven platform design is the rapid spread of misinformation and harmful narratives. Algorithmic systems designed to prioritize engagement may inadvertently promote misleading or inaccurate information if such content generates high levels of user interaction.

In the context of children's digital experiences, misinformation may include false health advice, conspiracy theories, or distorted representations of social issues. Young users who lack the skills or experience to critically evaluate online information may be particularly vulnerable to such content.

Moreover, algorithmic systems may amplify communities or networks that promote harmful behaviors, including harassment campaigns, extremist narratives, or discriminatory ideologies. While platforms have introduced moderation policies aimed at reducing harmful content, enforcement challenges remain significant given the scale and speed at which information circulates online.

Civil society organizations have therefore emphasized the importance of transparency and accountability in the design and operation of algorithmic systems. Without greater transparency regarding how recommendation algorithms function, it remains difficult for regulators, researchers, and the public to assess their impact on user well-being and democratic discourse.

6.5. Implications for children's rights

The structural drivers of digital harm described above have important implications for the protection of children's rights in the digital environment. The Convention on the Rights of the Child recognizes that children are entitled not only to protection from harm but also to privacy, freedom of expression, access to information, and participation in cultural and social life.

When digital platforms are designed in ways that prioritize data extraction and attention capture, these rights may be affected. Extensive data collection practices may undermine children's right to privacy. Algorithmic amplification of harmful content may expose children to material that affects their well-being or development. Engagement-driven design features may contribute to patterns of digital dependency that affect mental health.

From a human rights perspective, addressing these challenges requires more than restricting children's access to digital technologies. It requires examining the structural incentives that shape how platforms operate and how digital environments are designed.

6.6. Toward structural regulation of digital platforms

Recognizing the structural drivers of digital harm has led many policymakers and human rights advocates to call for regulatory approaches that address the responsibilities of technology companies themselves. Such approaches may include requirements for platforms to conduct human rights impact assessments of their technologies, transparency obligations regarding algorithmic systems, restrictions on targeted advertising directed at minors, and stronger protections for children's personal data.

Regulators may also consider age-appropriate design standards requiring platforms to prioritize safety and well-being in products used by children. These standards could include limits on addictive design features, clearer privacy protections, and enhanced reporting mechanisms for harmful content.

Ultimately, protecting children in digital environments requires a shift in regulatory focus. Instead of treating children's presence online as the primary source of risk, policymakers must recognize that many harms arise from the structure and incentives of the digital ecosystem itself. Addressing these structural drivers is therefore essential for creating digital environments that respect children's rights, support their development, and ensure that technological innovation advances in ways that are consistent with human dignity and human rights.

7. Legal Framework in Lebanon

Recent developments in Lebanon demonstrate growing recognition of the need to address risks associated with children's use of digital technologies.

While several laws provide partial protections relevant to children in digital environments, Lebanon currently lacks a comprehensive regulatory framework addressing children's access to social media platforms.

7.1. Cabinet Initiative to Develop a National Strategy

The issue of children's access to the internet and social media platforms in Lebanon has recently been addressed through emerging legislative and policy initiatives. On 26 February 2026, the Lebanese Council of Ministers adopted Decision No. 13 (Minutes No. 52), approving the formation of a joint ministerial committee tasked with preparing a comprehensive national strategy to regulate and guide the use of the internet and digital applications by children. The decision was adopted following a proposal submitted by the Ministry of Information and is grounded in several existing legal instruments, including the Lebanese Penal Code (Legislative Decree No. 340/1943), the Law on the Protection of Juveniles in Conflict with the Law or at Risk (Law No. 422/2002), the Law on the Protection of Women and Other Family Members from Domestic Violence (Law No. 293/2014), and the Law on Electronic Transactions and Personal Data (Law No. 81/2018). The Cabinet decision recognizes that, while these laws provide partial protection in the digital sphere, Lebanon lacks a comprehensive policy or regulatory framework addressing the risks associated with children's use of the internet and social media. It therefore mandates the establishment of an inter-ministerial committee composed of the Ministers of Information, Justice, Telecommunications, Social Affairs, Technology and Artificial Intelligence, Education and Higher Education, Interior and Municipalities, and Environment, in addition to the head of the national team responsible for combating cybercrime and the President of the National Human Rights Commission. The committee is tasked with developing a national plan to guide and regulate children's use of internet platforms and applications, in coordination with relevant public institutions, civil society actors, and international organizations such as UNICEF. This initiative is framed within Lebanon's obligations under international human rights law, particularly the Convention on the Rights of the Child, which Lebanon ratified in 1990 and which requires the state to take appropriate measures to ensure the protection and best interests of the child, including in the digital environment.

The committee includes representatives from multiple ministries, the national cybercrime unit, and the President of the National Human Rights Commission.

7.2. Draft Law on Prohibiting the Use of Social Media by Minors

The draft law proposed by Member of Parliament Tony Frangieh on 25 February 2026 seeks to establish a legal framework regulating children's access to social media platforms in Lebanon. The proposal defines a minor as any person under the age of fourteen and prohibits social media platforms from creating or activating accounts for individuals below this age threshold. It requires service providers operating within Lebanon to adopt effective and privacy-respecting age verification mechanisms, including parental verification systems, digital age verification tools, or artificial intelligence-based technologies to ensure compliance with the minimum age requirement. The draft law also introduces safeguards aimed at protecting minors' personal data, prohibiting platforms from collecting, exploiting, or selling children's data for commercial or media purposes. Enforcement provisions include criminal sanctions for non-compliant platforms, ranging from three months to two years of imprisonment and fines between five and twenty times the official minimum wage, in addition to the possibility for the Ministry of Telecommunications to suspend platform operations partially or entirely in cases of repeated violations. The proposal provides limited exceptions for electronic learning platforms and educational communication applications and grants service providers a three month period following the publication of the law in the Official Gazette to comply with its provisions. Implementation measures are to be developed jointly by the Ministries of Telecommunications and Social Affairs. The accompanying explanatory memorandum highlights the growing risks associated with early exposure to social media, including cyberbullying, exposure to harmful content, online exploitation, and negative impacts on children's mental health, while emphasizing Lebanon's obligations under international law, particularly the Convention on the Rights of the Child, to ensure the protection of children in the digital environment.

8. Assessment of the Lebanese Proposal in Light of International Human Rights Standards

The draft law proposed in Lebanon to prohibit social media use by minors under the age of fourteen reflects legitimate concerns regarding the potential risks associated with children's exposure to digital platforms. These risks include cyberbullying, exposure to harmful content, online exploitation, and psychological harms associated with excessive digital engagement. Nevertheless, legislative initiatives regulating children's access to digital technologies must be assessed within the framework of international human rights law, particularly the standards articulated by the United Nations Committee on the Rights of the Child and other international bodies addressing children's rights in the digital environment.

8.1. Compatibility with the Convention on the Rights of the Child

The Convention on the Rights of the Child requires States Parties to ensure that children's rights are respected, protected, and fulfilled in all environments, including the digital sphere. The UN Committee on the Rights of the Child clarified these obligations in General Comment No. 25 on children's rights in relation to the digital environment, adopted in 2021. The Committee emphasized that the digital environment has become central to the realization of children's rights and that technological innovations affect children's civil, political, economic, social, and cultural rights in interconnected ways. [9]

General Comment No. 25 affirms that meaningful access to digital technologies can support children in exercising a wide range of rights, including the rights to education, access to information, freedom of expression, cultural participation, and social development. At the same time, the Committee recognizes that digital environments can expose children to significant risks, including exploitation, privacy violations, harmful content, and abusive conduct.

[9] UN Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc. CRC/C/GC/25, 2 March 2021. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Consequently, the Committee calls on states to adopt regulatory frameworks that both protect children from harm and enable them to benefit from digital technologies. Importantly, the Committee stresses that protective measures must respect the principles of proportionality, necessity, and the evolving capacities of the child. Blanket restrictions that entirely exclude children from digital environments may therefore raise concerns if they disproportionately limit children's rights to information, participation, and expression.

In the Lebanese context, the proposed age-based prohibition raises questions regarding whether a complete restriction on access to social media platforms for children under fourteen constitutes a proportionate response to the identified risks. While the protection of children is a legitimate objective under international law, states must demonstrate that restrictive measures are necessary and that less restrictive alternatives would not achieve the same protective objective.

8.2. Age Verification and Privacy Concerns

The draft law requires digital platforms to implement age verification mechanisms in order to prevent minors from creating accounts. While age assurance technologies may contribute to the protection of children online, international human rights bodies have highlighted the potential privacy risks associated with such mechanisms.

General Comment No. 25 stresses that the collection and processing of children's personal data in digital environments must respect the highest standards of privacy protection. States are required to ensure that digital service providers adopt privacy-by-design and data minimization principles when processing children's data.

Many age verification systems rely on the submission of sensitive personal data, including government-issued identification documents, facial recognition technologies, or biometric verification tools. These mechanisms may create new risks for children if personal data is stored or processed by private companies with inadequate safeguards.

Human rights organizations have therefore cautioned that age verification systems must be carefully designed to avoid unnecessary collection of personal data and to ensure compliance with international privacy standards. From a human rights perspective, age assurance measures should prioritize privacy-preserving technologies and independent oversight mechanisms to prevent misuse of children's personal information.

8.3. Structural Drivers of Harm in Digital Platforms

Another key issue concerns the underlying causes of many digital harms experienced by children. Research and policy analysis conducted by human rights organizations, including Amnesty International's technology and human rights programme, indicate that many risks associated with social media use are linked to the structural design of digital platforms rather than simply to children's presence online.

Many social media platforms rely on surveillance-based business models that depend on extensive data collection and algorithmic recommendation systems designed to maximize user engagement. These systems can amplify sensational or emotionally provocative content, which may include harmful or misleading material. As a result, users, including children, may be exposed to content that undermines their well-being or psychological health.

From this perspective, regulatory approaches focusing solely on restricting access for young users may fail to address the structural drivers of digital harm. International human rights experts increasingly argue that regulatory frameworks should focus on ensuring that digital platforms operate in ways that respect human rights, including children's rights.

Such frameworks may include requirements for algorithmic transparency, limits on targeted advertising directed at minors, and obligations for platforms to conduct human rights impact assessments of their technologies.

8.4. Children's Rights to Participation and Access to Information

International human rights law recognizes that children are active participants in social and civic life rather than passive recipients of protection. The Convention on the Rights of the Child affirms children's rights to express their views, access information, and participate in cultural and social activities.

In the digital era, social media platforms often serve as important spaces where young people engage in political debate, share experiences, and access educational resources. General Comment No. 25 therefore emphasizes that states must ensure that children can meaningfully participate in digital environments while being protected from harm.

Blanket restrictions on children's access to social media platforms may inadvertently limit opportunities for participation and engagement. For example, young people frequently use digital platforms to access information about public affairs, participate in social movements, and express views on issues affecting their communities.

Regulatory approaches should therefore aim to strike a balance between protection and participation. Rather than excluding children from digital spaces entirely, policymakers may consider measures that promote safer digital environments while preserving opportunities for children to exercise their rights.

8.5. Role of National Human Rights Institutions

General Comment No. 25 highlights the role of national human rights institutions in monitoring and protecting children's rights in the digital environment. The Committee recommends that national human rights institutions be empowered to receive complaints from children, investigate digital rights violations, and provide oversight regarding the implementation of policies affecting children online.

In Lebanon, the involvement of the National Human Rights Commission in the inter-ministerial committee established by the Council of Ministers represents an important step toward ensuring that children's digital rights are considered within a broader human rights framework.

National human rights institutions can play a critical role in assessing the human rights implications of proposed legislation, promoting public awareness of children's digital rights, and ensuring that regulatory frameworks are consistent with international standards.

8.6. Toward a Balanced Regulatory Approach

The Lebanese draft law reflects legitimate concerns regarding children's safety in digital environments. However, international human rights standards suggest that effective regulation should address both the risks associated with children's digital engagement and the responsibilities of technology companies.

A balanced regulatory framework may therefore combine several elements, including age-appropriate design standards for digital platforms, stronger protections for children's personal data, algorithmic accountability mechanisms, and digital literacy initiatives aimed at empowering children and parents to navigate digital environments safely.

Such an approach aligns with international human rights standards and recognizes that protecting children in the digital age requires cooperation among governments, technology companies, educators, and civil society organizations.

9. Strengthening the Legal Framework for Digital Safety and Cybercrime

The effective protection of children in digital environments requires not only policies addressing access to social media platforms, but also a comprehensive legal framework capable of responding to the broader challenges posed by cybercrime, digital evidence, and cross-border digital investigations. The global nature of online platforms means that many digital harms affecting children, including cyberbullying, online exploitation, harassment, and the dissemination of harmful content, frequently involve actors, platforms, and infrastructure located across multiple jurisdictions. As a result, national legal frameworks must increasingly operate within broader systems of international cooperation.

In this context, recent developments in international law have strengthened the regulatory architecture governing cybercrime and digital evidence. The adoption of the United Nations Convention against Cybercrime represents a significant step toward establishing a global legal framework for addressing crimes committed through information and communications technologies while ensuring that investigative measures respect human rights and fundamental freedoms.

9.1. The United Nations Convention against Cybercrime

On 24 December 2024, the United Nations General Assembly adopted the United Nations Convention against Cybercrime through Resolution 79/243. The Convention represents the first comprehensive global treaty specifically aimed at addressing crimes committed through information and communications technology systems. The adoption of the Convention reflects growing international recognition that cybercrime constitutes a major transnational challenge requiring coordinated international responses.

The Convention establishes a legal framework designed to strengthen the capacity of States to prevent, investigate, and prosecute cybercrime while facilitating international cooperation in the collection and exchange of electronic evidence. It seeks to harmonize national criminal legislation relating to cybercrime offences, develop investigative tools adapted to digital environments, and create mechanisms for cross-border cooperation among law enforcement authorities.

The treaty also recognizes that the investigation of cybercrime frequently requires access to digital evidence located outside the territorial jurisdiction of the investigating state. As a result, the Convention provides procedures aimed at facilitating international cooperation, including mutual legal assistance, information sharing, and mechanisms for obtaining electronic evidence stored abroad.

At the same time, the Convention emphasizes the importance of ensuring that investigative powers in the digital sphere are exercised in a manner consistent with international human rights law. It therefore includes provisions requiring States Parties to ensure that measures adopted to combat cybercrime respect fundamental rights and freedoms, including the right to privacy, freedom of expression, and due process guarantees.

9.2. Entry into Force and Signature Process

In accordance with Article 64 of the Convention, the treaty was opened for signature in Hanoi on 25 and 26 October 2025 and subsequently at United Nations Headquarters in New York until 31 December 2026. Article 65 further provides that the Convention will enter into force ninety days after the deposit of the fortieth instrument of ratification, acceptance, or accession.

Once in force, the Convention is expected to serve as a key international instrument governing cooperation in cybercrime investigations and the exchange of electronic evidence between states. It aims to strengthen international legal cooperation, develop procedural safeguards for digital investigations, and promote respect for human rights in the context of combating cybercrime.

For states facing increasing challenges related to digital crime, participation in the Convention may significantly enhance the ability of national authorities to investigate offences involving cross-border digital infrastructures.

9.3. Relevance of the Convention for the Protection of Children

The growing use of digital platforms by children has been accompanied by an increase in online harms affecting minors. These harms include cyberbullying, harassment, the distribution of harmful or exploitative content, online grooming, and other forms of digital abuse. Many of these offences involve actors operating across multiple jurisdictions or using digital infrastructure hosted in different countries.

International cooperation mechanisms therefore play a critical role in enabling national authorities to investigate and prosecute such crimes effectively. The United Nations Convention against Cybercrime aims to strengthen such cooperation by establishing shared procedural frameworks for digital investigations and evidence gathering.

In the context of children's protection, the Convention may contribute to improving law enforcement responses to offences involving the exploitation or abuse of children in digital environments. By facilitating access to digital evidence and enabling cross-border investigations, the treaty may enhance the ability of national authorities to identify perpetrators and protect victims.

At the same time, the Convention highlights the need for procedural safeguards ensuring that investigative powers exercised in the digital sphere do not undermine human rights. Investigations involving digital communications, surveillance technologies, or data interception must therefore comply with international human rights standards governing privacy, due process, and freedom of expression.

9.4. The Lebanese Legal Framework

At the national level, Lebanon has adopted several legislative measures relevant to the regulation of the digital environment. The most significant of these is Law No. 81 of 10 October 2018 on Electronic Transactions and Personal Data, which provides the principal legal framework governing electronic communications, electronic signatures, and aspects of personal data protection.

Law No. 81/2018 establishes rules governing electronic transactions, digital authentication mechanisms, and certain aspects of cybersecurity. It also introduces provisions addressing the protection of personal data processed through electronic systems. These provisions are intended to regulate the collection, storage, and processing of personal data by public and private entities operating in Lebanon.

While Law No. 81/2018 represents an important step toward regulating digital activities within the country, it does not fully address the broader challenges associated with cybercrime and digital investigations. In particular, the law does not establish a comprehensive framework for international cooperation in cybercrime investigations or the exchange of electronic evidence with foreign jurisdictions.

Moreover, the law was adopted before the recent acceleration of global policy debates concerning digital platform regulation, algorithmic accountability, and children's rights in digital environments.

As a result, additional legislative reforms may be necessary to ensure that Lebanon's legal framework remains aligned with evolving international standards.

9.5. Lebanon and the United Nations Convention against Cybercrime

Lebanon has not yet acceded to the United Nations Convention against Cybercrime. Accession to the treaty could contribute significantly to strengthening Lebanon's capacity to investigate and prosecute cybercrime while facilitating international cooperation in obtaining electronic evidence.

Participation in the Convention would allow Lebanese authorities to benefit from the treaty's mechanisms for mutual legal assistance and cross-border cooperation. This could be particularly important in cases involving digital offences that affect children and involve platforms or perpetrators located outside Lebanese territory.

Accession could also contribute to aligning Lebanon's legal framework with evolving international standards concerning digital justice, data protection, and human rights in the digital environment. The Convention emphasizes the need to ensure that cybercrime investigations respect fundamental rights and procedural safeguards, including protections for privacy and freedom of expression.

For Lebanon, adopting such standards could strengthen both national cybercrime responses and broader efforts to regulate digital platforms in ways that protect users, including children, from harm.

9.6. Integrating Cybercrime Regulation into Child Protection Policies

Addressing online risks affecting children requires an integrated approach combining criminal law enforcement, platform regulation, data protection safeguards, and educational initiatives promoting digital literacy. Cybercrime legislation alone cannot fully address the complex challenges posed by children's engagement with digital technologies. However, effective legal frameworks for investigating digital offences remain an essential component of broader strategies aimed at protecting children online.

Strengthening Lebanon's legal capacity to address cybercrime may therefore complement other policy initiatives, including the development of national strategies regulating children's use of digital technologies and the promotion of safer online environments.

By aligning domestic legislation with international legal instruments such as the United Nations Convention against Cybercrime, Lebanon may enhance its ability to combat digital offences while ensuring that regulatory responses remain consistent with international human rights standards.

9.7. The Protection of Women from Digital and Online Violence

A Draft Law on the Protection of Women from Digital Violence was submitted to the Lebanese Parliament on 25 February 2026. The proposal was prepared with the support of the civil society organization "FEMALE" and introduced in Parliament by several Members of Parliament, including Bilal Abdallah, Paula Yacoubian, Jamil El-Sayyed, Tony Frangieh, Nada Boustani, Halima Kaakour, Saji Attieh, and Michel Douaihy. The draft law aims to establish a comprehensive legal framework to prevent, criminalize, and respond to different forms of technology-facilitated violence targeting women. It provides a broad definition of digital violence against women, encompassing acts committed through information and communication technologies that undermine women's dignity, privacy, psychological well-being, or security. The proposal criminalizes a range of offences including cyberstalking, online harassment, identity theft, electronic extortion, the non-consensual dissemination of intimate images, and the misuse of digital platforms to threaten, intimidate, or exploit women.

Beyond criminal sanctions, the proposal introduces protection mechanisms for victims, including judicial protection orders, accessible reporting mechanisms, and the provision of legal, social, and psychological support services. It also establishes preventive and institutional measures aimed at strengthening coordination between law enforcement authorities, judicial institutions, and civil society organizations, while promoting awareness and prevention strategies to address gender-based digital violence. The draft law therefore represents a significant legislative effort to address emerging forms of online gender-based violence and to enhance the protection of women's rights in Lebanon in line with international human rights standards.

Although the Draft Law on the Protection of Women from Digital Violence (2025) primarily aims to address technology-facilitated violence against women, several of its provisions indirectly contribute to strengthening protections for children and adolescents in the digital environment. The law establishes a broad legal framework addressing forms of online abuse, harassment, and exploitation that frequently affect minors as well as adult women.

First, the draft law criminalizes a range of online behaviors such as cyberstalking, online harassment, identity theft, electronic extortion, and the non-consensual dissemination of images or personal data. These acts are among the most common forms of digital harm experienced by children and

adolescents, particularly girls. By criminalizing such conduct and imposing penalties on perpetrators, the proposed legislation contributes to deterring harmful behavior in online spaces and enhancing accountability for technology-facilitated abuse.

Second, the law introduces protective judicial measures, including the possibility for victims to obtain protection orders and access support services. These mechanisms are particularly relevant for children who may be victims of online bullying, grooming, or digital exploitation. The availability of legal remedies and reporting procedures can help ensure that minors affected by digital violence receive timely protection and assistance.

Third, the proposal promotes institutional coordination and awareness-raising efforts among public authorities, law enforcement agencies, and civil society organizations to prevent digital violence. Such preventive measures are essential for protecting children in the digital environment, as they encourage safer online practices, improve reporting mechanisms, and strengthen institutional responses to online harm.

Finally, the law recognizes the broader societal risks associated with the misuse of digital technologies and emphasizes the need for policy responses that safeguard dignity, privacy, and personal security in online spaces. These principles align with international human rights standards, including the Convention on the Rights of the Child, which obliges states to protect children from all forms of violence, exploitation, and abuse, including those occurring through digital technologies.

Taken together, while the draft law is primarily framed around the protection of women, its provisions contribute to the broader objective of protecting vulnerable groups, including children, from technology-facilitated violence, thereby supporting the development of a safer and more accountable digital environment in Lebanon.

10. Strengthening the Legal Framework for Artificial Intelligence Regulation in Lebanon

Recent legislative and policy developments in Lebanon indicate growing recognition among policymakers of the need to regulate emerging digital technologies, particularly artificial intelligence, and to address their implications for human rights, privacy, digital governance, and the protection of children in online environments. As digital platforms, algorithmic systems, and generative artificial intelligence tools increasingly shape communication, economic activity, and public administration, Lebanese authorities have begun exploring institutional and legislative mechanisms capable of governing these technologies.

Taken together, these initiatives illustrate the gradual emergence of a national regulatory framework addressing digital harms, artificial intelligence governance, and the broader transformation of Lebanon's digital ecosystem. However, the current landscape remains fragmented, and the effectiveness of these initiatives will depend on the development of coherent legal safeguards aligned with international human rights standards.

10.1. Emerging Policy Frameworks for Digital Governance

In February 2026, the Lebanese Council of Ministers adopted Decision No. 13 (Minutes No. 52) establishing an inter-ministerial committee tasked with developing a comprehensive national strategy to guide and regulate children's use of the internet and digital applications. The initiative, proposed by the Ministry of Information, reflects growing concern regarding the impact of digital technologies on children and the risks associated with online environments.

The Cabinet decision acknowledges that although several Lebanese laws provide partial protections relevant to digital activities, Lebanon currently lacks a comprehensive regulatory framework governing children's use of digital platforms and emerging technologies.

Existing legal instruments referenced in the decision include:

- The Lebanese Penal Code (Legislative Decree No. 340 of 1943)
- The Law on the Protection of Juveniles in Conflict with the Law or at Risk (Law No. 422 of 2002)
- The Law on the Protection of Women and Other Family Members from Domestic Violence (Law No. 293 of 2014)
- The Law on Electronic Transactions and Personal Data (Law No. 81 of 2018).

While these instruments provide certain safeguards, they were adopted prior to the rapid expansion of digital platforms and artificial intelligence technologies and therefore do not comprehensively address contemporary digital governance challenges.

The Cabinet decision also emphasizes Lebanon's obligations under the Convention on the Rights of the Child, which requires states to ensure the protection and best interests of children in all environments, including digital spaces.

10.2. Legislative Initiatives Addressing Social Media Risks

Parallel to these policy initiatives, Lebanese lawmakers have introduced legislative proposals aimed at addressing specific digital risks affecting children.

One such proposal submitted on 25 February 2026 by Member of Parliament Tony Frangieh seeks to prohibit the use of social media platforms by minors under the age of fourteen. The proposal requires digital platforms operating in Lebanon to implement mechanisms verifying users' age and preventing minors from creating accounts.

The draft law also introduces provisions aimed at strengthening the protection of minors' personal data by prohibiting the commercial exploitation or unauthorized collection of children's personal information.

The proposal reflects growing concerns regarding the potential harms associated with early exposure to social media platforms, including cyberbullying, exposure to harmful or inappropriate content, and online exploitation.

However, as noted earlier in this report, such restrictions also raise complex policy questions regarding proportionality, effectiveness, and compatibility with international human rights standards relating to freedom of expression and access to information.

10.3. Addressing Artificial Intelligence-Generated Harms

Beyond social media regulation, Lebanese lawmakers have also begun addressing emerging harms associated with artificial intelligence technologies.

A draft law introduced in 2026 titled "Draft Law Criminalizing the Creation, Modification, or Use of Intimate or Indecent Images and Videos Generated or Altered by Artificial Intelligence without the

Consent of the Person Concerned" seeks to address the growing problem of synthetic audiovisual manipulation commonly known as deepfakes.

The proposal, introduced by Member of Parliament Anan Abdallah and other members of Parliament, criminalizes the creation, modification, or dissemination of artificial intelligence-generated content depicting individuals in intimate or degrading situations without their explicit consent.

The proposed legislation establishes liability for individuals who produce, distribute, or facilitate the circulation of such manipulated content through digital platforms. Importantly, it also extends liability to developers or providers of artificial intelligence tools that are intentionally designed for abusive purposes or knowingly used to produce harmful content.

The draft law introduces penalties including imprisonment, financial fines, and the confiscation of devices or software used to commit the offence. It also establishes aggravated sanctions in cases where the victim is a minor or where manipulated content is widely disseminated through digital platforms, recognizing the heightened harm that such acts may cause to vulnerable individuals.

10.4. Institutional Development of Artificial Intelligence Governance

Alongside legislative efforts addressing specific digital harms, Lebanon has also begun considering broader institutional mechanisms for governing artificial intelligence technologies.

In September 2025, the Lebanese Council of Ministers approved a draft law establishing the Ministry of Information Technology and Artificial Intelligence (MITAI). The initiative seeks to transform the existing State Ministry for Technology and Artificial Intelligence into a fully-fledged ministry responsible for coordinating Lebanon's national digital transformation strategy.

The initiative, led by Minister Kamal Shehadeh, aims to strengthen Lebanon's digital infrastructure, develop regulatory frameworks governing artificial intelligence technologies, and promote technological innovation across both public administration and the private sector.

According to the draft law transmitted to Parliament pursuant to Decree No. 12867 of 19 September 2025, the proposed ministry would be responsible for:

- developing national strategies for digital technologies and artificial intelligence
- supervising the national digital ecosystem
- strengthening cybersecurity policies

- protecting personal data
- supporting digital innovation and entrepreneurship.

The draft legislation also envisages the creation of specialized directorates responsible for implementing national digital governance policies, including:

- a Directorate for Technology and Artificial Intelligence
- a Directorate for Cybersecurity and Data Protection
- a Directorate for the Digital Economy and Entrepreneurship.

If adopted, the creation of MITAI would represent a major institutional step toward consolidating digital governance responsibilities within a dedicated governmental authority.

10.5. Proposal for a National Artificial Intelligence Authority

In parallel with these institutional initiatives, Lebanese lawmakers have proposed the establishment of an independent regulatory authority dedicated to artificial intelligence governance.

On 4 June 2025, Members of Parliament Edgar Traboulsi, Gebran Bassil, Georges Atallah, Cesar Abi Khalil, Nicolas Sehnaoui, and Jimmy Jabbour submitted a Draft Law on the Establishment of the National Artificial Intelligence Authority.

The proposed authority would function as an independent national body responsible for developing and overseeing Lebanon’s national strategy for artificial intelligence.

According to the draft law, the authority would be tasked with:

- preparing the national strategy for the artificial intelligence sector
- proposing regulatory frameworks governing AI technologies
- monitoring the implementation of AI policies
- supervising the ethical and responsible use of artificial intelligence
- proposing legislative reforms where necessary.

The authority would also report periodically to the Council of Ministers through the Minister of Telecommunications.

The proposed institutional structure includes representatives from government institutions, the information technology and artificial intelligence sector, and civil society organizations specializing in digital technologies.

The draft law emphasizes the importance of aligning artificial intelligence development with Lebanon's broader legislative and public policy objectives, including transparency, access to information, technological innovation, and responsible governance.

It also highlights the need to strengthen national capacities in education, research, and technological development to ensure that Lebanon can benefit from the opportunities presented by artificial intelligence while mitigating potential risks to society and fundamental rights.

10.6. Civil Society Concerns and Digital Sovereignty

Alongside governmental initiatives, Lebanese civil society organizations have expressed concerns regarding the governance implications of ongoing digital transformation efforts.

The digital rights organization SMEX (Social Media Exchange) has closely monitored developments relating to artificial intelligence governance and digital infrastructure in Lebanon. Civil society organizations have raised concerns regarding transparency, data protection, and the risks associated with reliance on foreign technology providers.

In particular, SMEX has warned that reliance on external technology providers for national digital infrastructure may pose risks to Lebanon's digital sovereignty and the protection of citizens' personal data.

These concerns were amplified following the announcement in December 2025 of an agreement with the technology company Oracle to provide artificial intelligence training to approximately 50,000 participants in Lebanon. While the government emphasized that the agreement does not grant foreign companies access to public sector data, civil society organizations expressed concern that insufficient regulatory safeguards could expose sensitive information to external actors.

Observers have also highlighted shortcomings in Lebanon's existing data protection framework. Although Law No. 81 of 10 October 2018 on Electronic Transactions and Personal Data provides a legal foundation for regulating personal data processing, it has not yet been fully implemented and lacks strong independent oversight mechanisms.

Civil society organizations have therefore called for stronger institutional safeguards to ensure transparency in digital governance, accountability in public-private technology partnerships, and effective protection of personal data.

10.7. Toward a Rights-Based Artificial Intelligence Governance Framework

Taken together, these initiatives demonstrate that Lebanon has begun to develop an institutional and legislative framework addressing the challenges posed by artificial intelligence and digital technologies.

However, the current regulatory landscape remains fragmented and requires further consolidation in order to ensure coherent governance.

Developing an effective regulatory framework for artificial intelligence will require addressing several key issues, including:

- protection of privacy and personal data
- accountability for algorithmic decision-making systems
- safeguards against digital harassment and AI-generated manipulation
- protection of children in digital environments
- transparency and oversight in the use of AI technologies by public authorities.

Ensuring that digital governance frameworks incorporate these safeguards will be critical to ensuring that technological innovation in Lebanon develops in a manner consistent with human rights, democratic governance, and the protection of vulnerable individuals in the digital age.

11. Recommendations and Outcomes

In light of the findings of this report, the Lebanese National Human Rights Commission, including the Committee for the Prevention of Torture, should call for a coordinated, rights-based national approach to digital governance that protects children, safeguards privacy, strengthens accountability for digital platforms and artificial intelligence systems, and aligns Lebanon's laws and institutions with international human rights standards. The recommendations below are directed to the Lebanese Government, the Lebanese Parliament, relevant ministries and public authorities, civil society organizations, and United Nations agencies and treaty bodies.

The NHRC-CPT should position itself as a central independent actor in Lebanon's emerging digital rights framework. It should issue formal opinions on draft laws, monitor their human rights impact, engage with ministries and Parliament, and advocate for child-sensitive, privacy-respecting, and rights-based digital regulation. It should also explore mechanisms for receiving and documenting complaints related to digital harms affecting children and other vulnerable groups.

Through this role, the NHRC-CPT can help ensure that Lebanon's response to social media risks, cybercrime, and artificial intelligence is not driven solely by security or moral panic, but by principled adherence to human dignity, the rule of law, and international human rights obligations.

11.1. Recommendations to the Lebanese Government

The Government of Lebanon should adopt a whole-of-government national strategy on children's rights in the digital environment, ensuring that all regulatory initiatives affecting children's access to digital technologies are guided by the best interests of the child, the principles of legality, necessity, and proportionality, and the obligation to protect children while preserving their rights to expression, information, education, participation, and privacy.

The Council of Ministers should ensure that the inter-ministerial committee established by Decision No. 13 of 26 February 2026 operates transparently, includes meaningful consultation with children, parents, teachers, child protection specialists, digital rights experts, and civil society organizations, and produces a public national strategy with clear objectives, timelines, and institutional responsibilities. The Government should also ensure that the National Human Rights Commission plays a substantive and independent oversight role in this process.

The Government should refrain from adopting blanket digital restrictions affecting children unless it can demonstrate that such measures are strictly necessary, proportionate, evidence-based, and accompanied by robust safeguards for children's rights. Instead, priority should be given to regulatory measures targeting the structural drivers of online harm, including unsafe platform design, opaque algorithmic systems, exploitative data practices, and weak complaint and remedy mechanisms.

The Government should initiate the accession process to the United Nations Convention against Cybercrime, while ensuring that any implementing measures fully comply with international human rights law, particularly protections for privacy, freedom of expression, due process, and judicial oversight. It should also update domestic legislation to regulate cybercrime investigations, cross-border electronic evidence, and digital procedural safeguards in a manner consistent with human rights standards.

The Government should accelerate the implementation and reform of Law No. 81/2018 on Electronic Transactions and Personal Data by establishing effective enforcement mechanisms and independent oversight for personal data protection, particularly in relation to children's data, biometric data, and age verification systems.

In the area of artificial intelligence, the Government should ensure that any future ministry, authority, or regulatory mechanism tasked with AI governance is established on the basis of independence, transparency, public accountability, and human rights compliance. AI governance should include mandatory safeguards against discrimination, unlawful surveillance, privacy violations, and AI-generated harms such as non-consensual deepfakes and manipulative synthetic media.

11.2. Expected outcomes from government action

• Adopting a comprehensive national strategy on children's rights in the digital environment based on international human rights standards, ensuring the protection of children while safeguarding their fundamental rights to expression, participation, access to information, and privacy.

• Developing a coherent national framework for digital governance that coordinates policies related to online child protection, regulation of digital platforms, cybercrime prevention, personal data protection, and the governance of artificial intelligence.

• Strengthening Lebanon's capacity to investigate and prosecute digital crimes, particularly those targeting children, by aligning national legislation with international standards and enhancing international cooperation mechanisms related to digital evidence.

• Establishing an effective personal data protection system that includes clear enforcement mechanisms and independent oversight, with particular attention to the protection of children's data, biometric data, and age-verification systems.

• Adopting a human rights–based regulatory framework for artificial intelligence that ensures transparency and accountability and introduces safeguards to prevent discrimination, unlawful surveillance, and manipulation of digital content.

• Enhancing accountability and transparency in the operations of digital platforms and technology companies, including the adoption of rules related to safer platform design, limitations on targeted advertising to children, and strengthened complaint and remedy mechanisms.

• Supporting initiatives on digital literacy and empowerment for children, parents, and teachers to raise awareness of digital risks and promote the safe and responsible use of technology.

• Strengthening institutional coordination and cooperation among government entities, civil society, the private sector, and international organizations to develop balanced digital policies that protect rights while supporting technological innovation in Lebanon.

11.3. Recommendations to the Lebanese Parliament

The Lebanese Parliament should review all draft laws relating to social media, cybercrime, artificial intelligence, and digital governance through a human rights lens. In particular, Parliament should subject the draft law prohibiting social media use by minors under fourteen to careful scrutiny in light of the Convention on the Rights of the Child, General Comment No. 25, and Article 19 of the International Covenant on Civil and Political Rights.

Parliament should amend any proposal relying on intrusive age verification or broad platform sanctions unless such measures are narrowly tailored, privacy-preserving, and subject to independent oversight. Instead of relying primarily on prohibition, Parliament should legislate for age-appropriate design, stronger data protection for children, restrictions on targeted advertising to minors, and clear obligations on platforms to assess and mitigate risks to children's rights.

Parliament should adopt a modern and comprehensive legal framework for artificial intelligence that clearly regulates public and private uses of AI, provides remedies for victims of AI-generated harms, requires transparency and human rights due diligence, and establishes accountability for developers, deployers, and intermediaries.

Parliament should also consider the creation of an independent digital rights or data protection authority, or ensure that any proposed National Artificial Intelligence Authority has sufficient independence, expertise, and oversight powers, including the authority to receive complaints and investigate violations.

11.4. Expected outcomes from parliamentary action

• Ensuring that all legislation related to the digital environment, including the regulation of social media, cybercrime, and artificial intelligence, complies with international human rights standards, particularly the Convention on the Rights of the Child and the International Covenant on Civil and Political Rights.

• Developing a balanced legislative framework that protects children from digital risks without imposing disproportionate restrictions on their rights to freedom of expression, access to information, and participation in digital life.

• Strengthening the protection of children's personal data by establishing clear rules regarding data collection, processing, and use, and limiting targeted advertising to minors and exploitative digital practices.

• Adopting modern legislation regulating artificial intelligence that ensures transparency and accountability and provides remedies for individuals harmed by algorithmic systems or AI-generated content.

• Strengthening parliamentary oversight of digital policies by monitoring the implementation of national strategies related to digital governance and ensuring that government initiatives are subject to democratic accountability.

• Supporting the establishment of independent bodies for data protection or digital rights with sufficient expertise and authority to oversee compliance with digital laws and investigate violations.

• Strengthening public trust in digital policies and technology-related legislation by ensuring transparency, accountability, and respect for fundamental rights in the legislative decision-making process.

11.5. Recommendations to Ministries and Public Authorities

The Ministries of Information, Telecommunications, Justice, Social Affairs, Education and Higher Education, Interior and Municipalities, Technology and Artificial Intelligence, and other relevant authorities should coordinate closely to ensure that digital regulation is not approached solely as a technical or security issue, but also as a child protection, privacy, education, and human rights issue.

The Ministry of Education should develop digital literacy and online safety curricula tailored to different age groups, including modules on privacy, cyberbullying, misinformation, consent, online exploitation, and responsible use of artificial intelligence tools. The Ministry of Social Affairs should strengthen psychosocial support and reporting pathways for children affected by online harms. The Ministry of Justice should review procedural laws and criminal legislation to ensure effective remedies and fair processes in digital cases. The Ministry of Telecommunications should ensure that regulatory measures imposed on platforms are lawful, transparent, and rights-compliant.

Public authorities should also publish technology agreements, digital transformation plans, and AI-related partnerships affecting public services, subject to narrow exceptions justified by law, in order to guarantee transparency and public accountability.

11.6. Expected outcomes from ministerial action

• Strengthening institutional coordination among ministries and public authorities in regulating the digital space, ensuring a comprehensive approach that considers child protection, privacy, education, and human rights alongside technical and security considerations.

• Integrating digital literacy and online safety into national educational curricula, enabling children and young people to acquire the skills necessary for the safe and responsible use of digital technologies and artificial intelligence.

• Developing effective reporting and support mechanisms for children affected by digital harm, including psychological and social support services and clear pathways for reporting cyberbullying or online exploitation.

• Improving the procedural and legal framework for addressing digital crimes, ensuring the availability of effective remedies for victims and fair and efficient judicial procedures in cases related to the digital environment.

• Enhancing transparency and accountability in digital transformation policies and technology partnerships between the public and private sectors, including the publication of agreements and initiatives related to technology and artificial intelligence.

• Ensuring that regulatory measures imposed on digital platforms are lawful, clear, and consistent with human rights standards, while strengthening protections for users, particularly children.

• Building institutional capacities within ministries and public authorities to address challenges related to digital technologies and artificial intelligence, thereby strengthening the state's ability to develop balanced and sustainable digital policies.

• Strengthening public trust in governmental digital policies through transparency, accountability, and the protection of fundamental rights in the management of Lebanon's digital transformation.

11.7. Recommendations to Civil Society Organizations

Civil society organizations should continue monitoring legislative and policy developments affecting children's rights, digital governance, cybercrime regulation, and artificial intelligence in Lebanon. They should engage in evidence-based advocacy, contribute to public consultation processes, and provide independent expertise on privacy, digital rights, child protection, gender-based online violence, and digital sovereignty.

Organizations working with children and families should expand awareness campaigns on children's rights in the digital environment and create accessible reporting and support mechanisms for those exposed to online harm. Digital rights organizations should continue scrutinizing technology agreements, regulatory proposals, and institutional reforms, including the governance implications of foreign technology partnerships and AI training initiatives.

Civil society should also build coalitions across sectors, including child rights, media freedom, women's rights, disability rights, education, and technology policy, to ensure that digital governance debates are inclusive and rights-based.

11.8. Expected outcomes from civil society action

• Strengthening independent oversight of digital legislation and policies to ensure their alignment with international human rights standards and the protection of children in the digital environment.

• Raising public awareness of children's rights online and the risks associated with cyberbullying, digital exploitation, privacy violations, and misinformation.

• Developing effective reporting and support mechanisms for victims, particularly children and adolescents exposed to online harm or violence.

• Enhancing accountability and transparency in digital policies and technology partnerships between the public and private sectors, including agreements related to digital infrastructure or artificial intelligence programs.

• Providing independent expertise to decision-makers through research, studies, and public consultations related to digital governance, data protection, and artificial intelligence.

• Building broad coalitions among civil society organizations working in the fields of children's rights, media freedom, women's rights, education, and technology policy, thereby strengthening a comprehensive approach to digital governance.

• Strengthening civil society participation in the development of digital policies to ensure that these policies are inclusive and responsive to human rights considerations and the needs of the most vulnerable groups.

• Supporting the development of a safer, more equitable, and more accountable digital environment in Lebanon, enabling society to benefit from technological innovation while reducing its risks to individuals and communities.

11.9. Recommendations to UN Agencies and Treaty Bodies

UN agencies, including UNICEF, OHCHR, UNESCO, UNDP, and ITU, should provide coordinated technical assistance to Lebanon in the development of a national strategy on children's rights in the digital environment, digital literacy policies, privacy safeguards, and AI governance frameworks grounded in human rights.

UNICEF should support child-centered policy development and meaningful child participation in digital governance reform. OHCHR should provide guidance on the compatibility of proposed laws and policies with international human rights standards, including on privacy, expression, and the rights of the child. UNESCO should support ethical AI policy development and digital education. UNDP and other partners should assist with institutional capacity-building and regulatory design.

Treaty bodies, especially the Committee on the Rights of the Child and the Human Rights Committee, should continue to address Lebanon's digital governance obligations in their dialogues and concluding observations, including the regulation of children's online safety, data protection, cybercrime enforcement, and AI-related harms.

11.10. Expected outcomes from UN engagement

• Providing technical and methodological support to Lebanon in developing a comprehensive national strategy on children's rights in the digital environment and advanced policies for digital governance.

• Strengthening the alignment of Lebanese legislation and policies with international human rights standards, particularly the Convention on the Rights of the Child and the International Covenant on Civil and Political Rights.

• Supporting the development of educational policies on digital literacy and promoting children's and young people's skills for the safe and responsible use of technology and artificial intelligence.

• Strengthening the institutional capacities of the Lebanese government and national bodies in the areas of data protection, artificial intelligence regulation, and cybercrime prevention.

• Promoting the participation of children and young people in the development of digital policies to ensure that these policies reflect their needs and experiences in the digital environment.

• Developing ethical and regulatory frameworks for artificial intelligence based on the principles of transparency, accountability, and respect for human rights.

• Encouraging international cooperation and the exchange of expertise in the field of digital governance and the protection of children online.

• Supporting continuous international monitoring of digital developments in Lebanon through international treaty mechanisms, thereby strengthening compliance with Lebanon's human rights obligations.