



Republic of Tunisia
Ministry of Family, Women, Childhood & the Elderly

Institutional Assessment of the prevention and protection of children from online violence in Tunisia

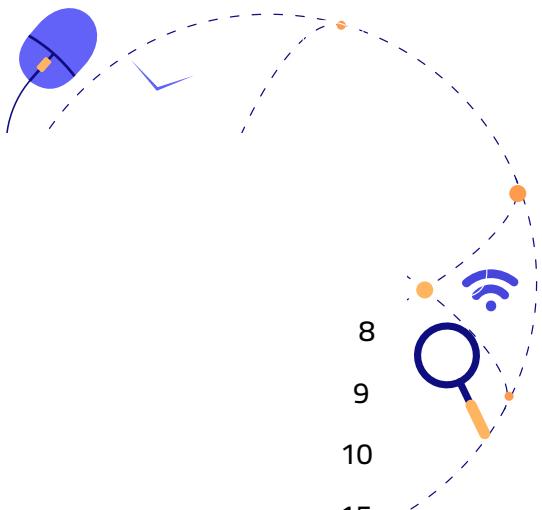


USAID
FROM THE AMERICAN PEOPLE

unicef 
for every child

Table of contents

- I- Acknowledgments 8
- II. Acronyms 9
- III. Glossary 10
- IV. Executive Summary 15
 - 1. Background 15
 - 2. Methodology 15
 - 3. Research findings 16
 - 3.1. Internet benefits and risks 16
 - 3.2. Prevention and response to online risks and harms 18
- V. Recommendations 20
 - 1. Policy and legislation 20
 - 1.1 Capacity-building and systems strengthening 20
 - 1.2. Prevention and response mechanisms 21
 - 1.3 Ensuring inter-government coordination on child online protection 21
- I. Introduction 23
 - 1. Background 23
 - 2. Study objectives 24
 - 3. Research Methodology 25
 - 4. Key Stakeholder Interviews 26
 - 5. Focus Group Discussions 27
 - 5.1. Focus Groups with children 28
 - 5.2. Focus Groups with parents 29
 - 5.3. Focus Groups with educators 30
 - 6. Ethics and child protection 30
 - 7. Data analysis 31
 - 8. Methodology limitations 31



II. Internet benefits and risks: A child-centric perspective	32
1. In moderation, internet use provides many educational, social, and economic benefits	32
2. Educational benefits	32
2.1. Enhancing academic learning	32
2.3. Social benefits: Maintaining and building social relations:	34
2.4. Entertainment	34
2.5. Commercial benefits and monetary gain	34
2.6. Mental Health benefits	35
3. Internet use is associated with new and enhanced physical, mental, and psychological risks and harms	36
3.1. Excessive Internet use	36
3.2. Bullying	37
3.3. Hacking	38
3.4. Sexual Harassment	38
3.5. Fake Profiles and Extortion	39
6.6. Normalizing violence and online radicalization	41
7.7. Mental Health risks	41
III. Prevention and response to online risks and harms facing children	42
1. Children's existing approaches to online protection	42
1.1. Active measures children take to protect themselves online	42
1.2. Help and knowledge seeking	43
1.3. Tailored and differentiated measures for protection	44
2. Existing efforts and measures for prevention and response	45
3. Legal and institutional gaps in online violence prevention and response	47
3.1. Legal gaps	48
3.2. Gaps in knowledge and capacity amongst key child protection actors	49
3.3. Lack of psychological support for children	50
IV. Recommendations	52

1. Recommendations on research and data	52
2. Policy and legislative recommendations	53
2.1. Ensuring consistency across instruments and laws	53
2.2. Prioritizing the reform of the Child Protection Code	54
2.3. Establishing Industry Guidelines for online child protection	55
3. Capacity building and systems strengthening	55
3.1. Training for Educators	55
3.2. Training for child and family judges	56
3.3. Digital literacy and COP training for public officials	56
3.4. Training on responsible child-rights focused reporting for journalists	57
4. Prevention and response mechanisms	57
4.1. Launching awareness campaigns targeting children and parents	57
4.2. Improving children's resilience to online risks and harms	59
4.3. Enhancing psycho-social support provision for children	60
5. Institutional recommendations	60
5.1. Ensuring inter-government coordination on child online protection	60
5.2. Integrating online protection into the formal child protection mechanism	61
List of Annexes	62

Appendix 1 : Literature Review	63
I. Introduction	64
1. Analytical approach	64
2. Limitations	64
II. Children online in Tunisia	65
III. Online Risks and Harms: Key Considerations	66
IV. Ending violence against children while protecting their rights	70
1. Children's vulnerability to online violence	71
2. Rights of the child	73
2.1. Right to protection against abuse	74
2.2. Access to justice	75

2.3. Data protection and confidentiality	76
V. International frameworks	77
1. International conventions applicable to Tunisia	78
2. Global Frameworks for Online Safety	80
2.1. INSPIRE Strategies: Seven Strategies to End Violence Against Children.	81
2.2. The National Response Model	82
2.3. Global guidelines for the digital industry	83

Annex 2: Mapping of the legal and institutional framework for online child protection in Tunisia	87
--	----

I. The legal framework for online child protection in Tunisia	88
1. Physical and moral integrity in the 2022 Constitution	88
2. Cyberviolence and electronic crimes in the penal code	88
3. Article 2001- 01 of January 15, 2001 promulgating the Telecommunications Code	91
4. Organic Law No. 26 of August 7, 2015 on Combating Terrorism and Preventing Money Laundering	91
5. Decree Law No. 115 - 2011 of November 2, 2011 on Freedom of the Press	92
6. Organic Law No. 58-2017 of August 22, 2017 on the Elimination of Violence against Women	93
7. Organic Law No. 61 of 2016 of August 3, 2016 on Preventing and Combating Trafficking in Persons	94
8. Child Protection Code	94
9. Law No. 2004-63 of July 27, 2004 on the Protection of Personal Data	95
10. Decree-Law No. 2022-54 of September 13, 2022, on the Fight against Crimes Relating to Information and Communication Systems	96
II. The institutional framework for online child protection in Tunisia	97
1. Police and National Guard Services:	97
1.1. Specialized units to investigate crimes of violence against women	97

1.2. The Juvenile Prevention Brigade	98
1.3. Anti-Human Trafficking Brigade:	99
1.4. The Social Welfare Sub-Directorate of the National Guard	99
1.5. The Technological Crime Brigade	99
2. Child Protection Officer (CPO)	99
3. Judicial authorities	100
3.1. The Family Judge	100
3.2. The Public Prosecutor's Office	100
3.3. The juvenile investigating judge	101
4. The National Authority for the Protection of Personal Data (INPDP)	101
5. National Body for Combating Trafficking in Persons (INLTP)	102
6. Coordination with educational institutions	102
7. IWF Tunisia Photo and Video Reporting Portal	103
Annex 3: Indicators for the selection of research sites	104
I. The regional development indicators	105
II. To the success of the baccalaureate	106
III. School drop-out rate	106

I- Acknowledgments

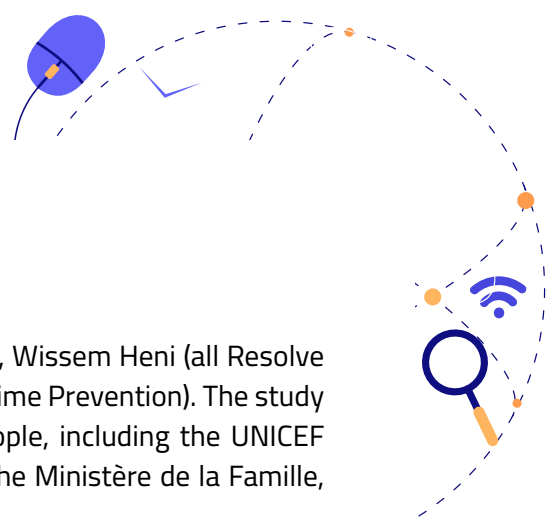
The report was written by Hanen Keskes, Alexander Martin, Wissem Heni (all Resolve Consulting) and Patrick Burton (the Centre for Justice and Crime Prevention). The study was only made possible through the support of many people, including the UNICEF Tunisia Country Office, who commissioned the work, and the Ministère de la Famille, de la Femme, de l'enfance et des seniors (MFFES).

In particular, the authors would like to extend their thanks to Antoine Deliege, Chadi Rabhi and Rabeb Ayari (UNICEF Tunisia Child Protection), and Ms. Jamila Bettaieb, Rami Ben Sallah and Samir Ben Meriem from the MFFES.

The authors would like to thank the many officials, civil society representatives and all other stakeholders who participated in the study and gave so generously of their time, as well as the project's steering committee.

The team owes a huge debt of gratitude to the children who gave up their time to speak so openly and honestly in the focus group discussions.

The NAP was made possible through a dedicated grant from the French National Committee of UNICEF and USAID. The findings and conclusions contained within the report are those of the Government of Tunisia and UNICEF and do not necessarily reflect the views of the French National Committee of UNICEF, USAID or the Governments of the United States.



II. Acronyms

ASD	Autism Spectrum Disorder
BEC	Listening and counseling offices (Les bureaux d'écoute et de conseil)
CEC	Listening and counseling cells (Les cellules d'écoute et de conseil)
CP	Child Protection
CNIPE	National Computer Center for Children (Centre National de l'informatique pour Child Online Protection)
CRC	Committee on the Rights of the Child
CSAM	Child Sexual Abuse Material
CPD	Child Protection Delegate review across all document
FG	Focus Group
GC	(CRC) General Comment
ICT	Information and Communication Technology
INTLP	National Authority for the Fight against Human Trafficking
IRB	Institutional Review Board
KSI	Key Stakeholder Interview
MFFES	Ministry of Family, Women, Children and Seniors
MNR	Model National Response
NAP	National Action Plan
OCSEA	Online child sexual exploitation and abuse
VAC	Violence against children

III. Glossary

Term	Definition
<p>Child</p> <p>Article 1, Convention on the Rights of the Child (CRC), 1989</p>	<p>Any human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier</p>
<p>Child sexual exploitation and abuse</p> <p>Article 18, Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)</p> <p>ECPAT. Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Adopted by the Interagency Working Group in Luxembourg, 28 January 2016</p> <p>See also: Committee on the Rights of the Child, Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, 10 September 2019</p>	<p>Child sexual abuse includes:</p> <p>(a) Engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities (this does not apply to consensual sexual activities between minors), and</p> <p>(b) engaging in sexual activities with a child where use is made of coercion, force or threats; or abuse is made of a recognized position of trust, authority or influence over the child, including within the family; or abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.</p> <p>Child sexual abuse becomes sexual exploitation when a second party benefits monetarily, through sexual activity involving a child. It includes harmful acts such as sexual solicitation and sexual exploitation of a child or adolescent in prostitution and, in the Council of Europe Convention, covers situations in which a child or other person is given or promised money or other form of remuneration, payment or consideration in return for the child engaging in sexual activity, even if the payment/ remuneration is not made.</p> <p>Although the terms are sometimes used interchangeably, what distinguishes the concept of child sexual exploitation from child sexual abuse is the underlying notion of exchange, financial or otherwise.</p>

<p>Child sexual abuse material</p> <p>Committee on the Rights of the Child, Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, 10 September 2019, para 60</p>	<p>Child sexual abuse material is covered under article 2 of the Optional Protocol to the CRC on the sale of children, child prostitution and child pornography as 'child pornography', and is defined as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes (art. 2 (c)).</p> <p>The Committee on the Rights of the Child recommends that States' parties, in line with recent developments, avoid the term 'child pornography' to the extent possible and use other terms such as the 'use of children in pornographic performances and materials', 'child sexual abuse material' and 'child sexual exploitation material'.</p>
<p>Cyberbullying</p>	<p>An intentional pattern of hurtful behaviour which typically involves elements of power imbalance, inflicted through the use of computers, cell phones and other digital devices. Cyberbullying may overlap with offline bullying.</p>
<p>Digital Education</p>	<p>Any teaching or learning processes that entail the use of digital technology, including online and offline formats, using distance, in-person, or hybrid approaches.</p>
<p>EdTech</p>	<p>Education technology (EdTech) refers to the practice of using technology to support teaching and the effective day-to-day management of educational institutions. It includes hardware (such as tablets, laptops or other digital devices), and digital resources (such as platforms and content), software and services that aid teaching, meet specific needs, and help the daily running of educational institutions.</p>

<p>Hacking</p>	<p>Use of technology to “gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating, or violence.”¹</p>
<p>Helpline</p>	<p>Helplines provide confidential advice and assistance to callers, often acting as points of referral to other service providers.</p>
<p>Hotline/Online reporting portal</p>	<p>A dedicated online reporting mechanism to report Internet material suspected to be illegal, including child sexual abuse material. A hotline enables the public to anonymously report online material they suspect may be illegal. A Hotline/ Online reporting portal is distinct from a Helpline (see above).</p>
<p>(Technology-facilitated) Image-Based Sexual Abuse</p>	<p>The non-consensual creation and/or distribution and/or threat of distribution of private, sexual images. Image-based sexual abuse may be used to describe a range of non-consensual offences involving the creation and dissemination of private sexual images, including revenge pornography, upskirting, deepfake media production, and cyber-flashing. It also includes image-based sexual harassment, which refers to the unsolicited sharing of sexual images.</p>
<p>Online harassment and online sexual harassment</p>	<p>Repeatedly contacting, annoying, threatening or scaring another person, either by an individual or a group. Online sexual harassment features uninvited sexual attention and sexual coercion.²</p>
<p>Online solicitation (or grooming) of a child for sexual purposes</p> <p>From UNICEF, 2020. Action to end child sexual abuse and exploitation: A review of the evidence, UNICEF, New York</p>	<p>Online solicitation of the child for sexual purpose. The process of establishing or building a relationship with a child through the internet or other digital technologies to facilitate child sexual abuse or exploitation.</p>

1 VAW Learning Network (2013). Technology-related Violence Against Women. Available at: https://www.vawlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html

2 N. Henry and A. Powell (2018) Technology-facilitated sexual violence: a literature review of empirical research. Trauma, Violence & Abuse, vol. 19, No. 2, pp. 195–208. <https://doi.org/10.1177/1524838016650189>

<p>Personal data</p>	<p>Any information relating to an individual child which allows them to be identified directly from that information or indirectly when there is additional information.³</p>
<p>Prevention</p> <p>World Health Organization (WHO), World Report on Violence and Health, WHO, Geneva, 2002.</p>	<p>Follows the WHO definition of 'primary prevention':</p> <p>Stopping child sexual abuse and exploitation before it occurs</p>
<p>Sexual violence</p>	<p>An umbrella term used here to refer to all forms of sexual victimization of adult women and of children – child sexual abuse and exploitation, rape and other sexual assaults, sexual harassment, abuse in pornography, prostitution and trafficking, FGM/C. Any sexual act, attempt to obtain a sexual act, unwanted sexual comments or advances, or acts to traffic, etc. directed at a person's sexuality using coercion, by any person, regardless of their relationship to the victim, in any setting, including but not limited to home and work.⁴</p>

³ Day, E. (2021). Governance of data for children's learning in UK state schools. Digital Futures Commission, 5Rights Foundation.
⁴ Krug EG, Mercy JA, Dahlberg LL, Zwi AB. (2002) The world report on violence and health. Lancet. 5;360(9339):1083-8. <https://pub-med.ncbi.nlm.nih.gov/12384003/>

Technology industry

ITU. Guidelines for industry on Child Online Protection, 2020

The ICT or technology sector covers a broad range of companies including but not limited to:

(a) Internet Service Providers (ISPs), including through fixed landline broadband services or cellular data services of mobile network operators: while this typically reflects services offered over a more long-term basis to subscribed customers, it could also be extended to businesses that provide free or paid public WI-FI hotspots.

(b) Social networks /messaging platforms and online gaming platforms.

(c) Hardware and software manufacturers, such as providers of handheld devices including mobile phones, gaming consoles, voice assistance-based home devices, Internet of Things and smart Internet connected toys for children.

(d) Companies providing digital media (content creators, providing access to or hosting content).

(e) Companies providing streaming services, including live streams.

(f) Companies offering digital file storage services, cloud-based service providers.

Violence against children

Article 19, Convention on the Rights of the Child (CRC), 1989

All forms of physical or mental violence, injury and abuse, neglect or negligent treatment, maltreatment or exploitation, including emotional violence and sexual abuse.

IV. Executive Summary

1. Background

Information and communication technologies (ICTs) have become central to children's everyday lives. While access to this technology provides numerous educational and social benefits to children, it also has the potential to expose them to risk and cause harm. Furthermore, it is possible for both risks and harms to traverse the digital and physical environments, whereby online risks can become offline harms and vice versa. To support the Ministry of Women, the Family, Children and Seniors (MFFES) strengthen the capacity of relevant sectors to address the types of vulnerabilities and violence against children in the virtual world, Resolve Consulting and the Centre for Justice and Crime Prevention (CJCP), with funding and support from UNICEF (Tunisia Office) conducted this research project aimed to support the Government of Tunisia to strengthen its capacity to prevent, detect and respond to violence against children. The findings will be used to inform the development of a national action plan (NAP) to combat online violence against children.

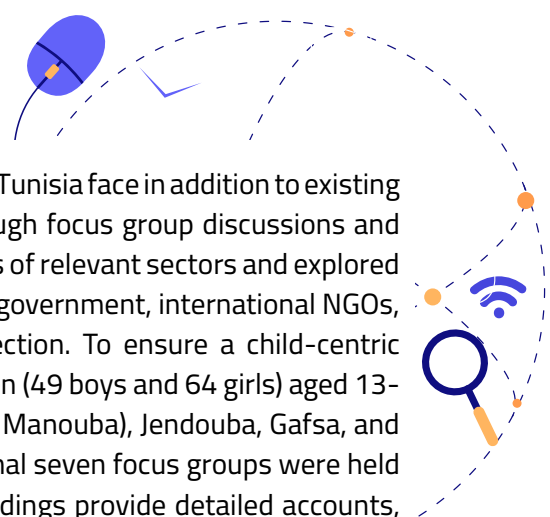
In order to achieve this outcome, the study set out to answer a series of questions:

- What are children's online experiences and knowledge and capacities regarding their rights and protection online?
- To what extent are protection against online violence in all forms and the promotion of online safety in all its forms integrated into legislation and policy in Tunisia?
- To what extent are different sectors within government, civil society and industry aware of their roles and responsibilities to prevent and respond to online violence against children?
- What are the existing structural and organizational measures and coordination mechanisms that ensure an intersectoral response to the prevention of online violence against children in Tunisia?
- What are the barriers that exist for a cross-sectoral response to and in preventing and responding to online violence against children in Tunisia, and how can they be addressed?

2. Methodology

The design of the study and analysis of the findings were framed within the context of the UN Committee on the Rights of the Child's General Comment No.25 on the Rights of the Child in the Digital Environment, the We Protect Model National Response (MNR), and the INSPIRE Strategies for ending Violence Against Children.

To answer the research questions, this research conducted a thorough mapping of the legal framework including Tunisian national laws and the international conventions on child protection signed by the Tunisian government. This was combined with a mapping of the institutional structures and mechanisms involved in the Online Child Protection landscape in Tunisia.


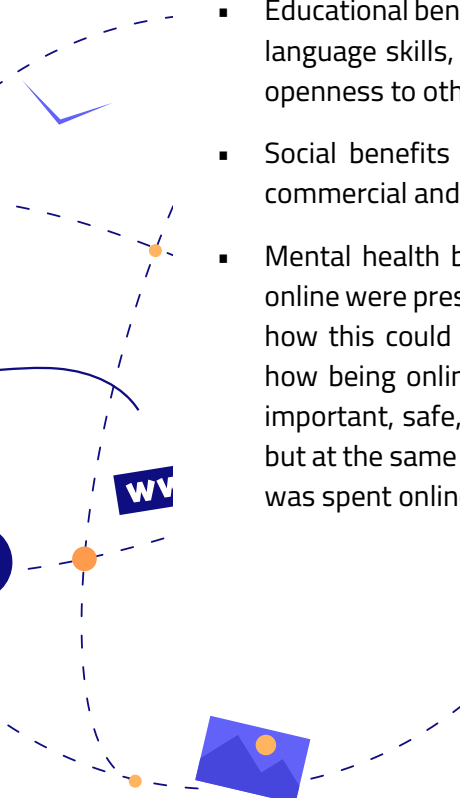


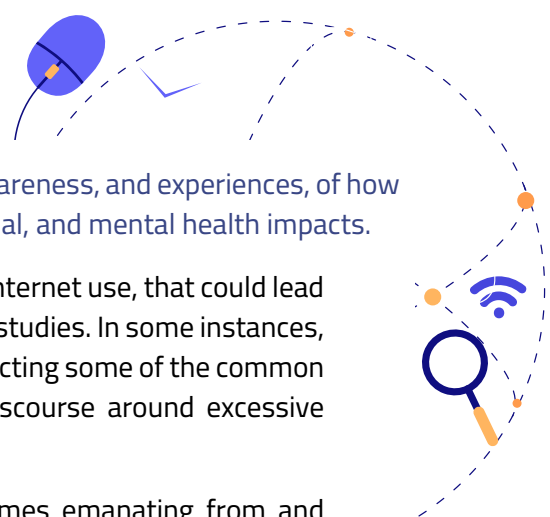
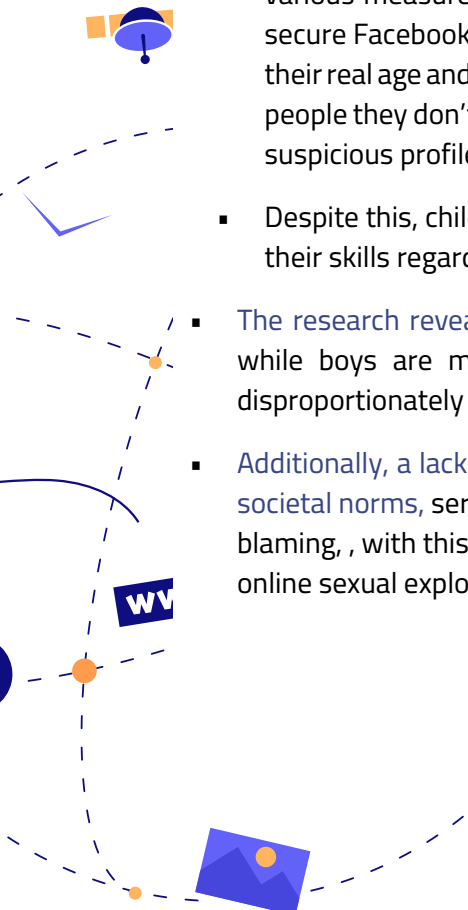
With a view to exploring the types of online violence that children in Tunisia face in addition to existing responses and gaps, the research collected qualitative data through focus group discussions and key stakeholder interviews. This assessed the needs and capacities of relevant sectors and explored children's online experiences. 17 Interviews were conducted with government, international NGOs, judicial, healthcare, and civil society actors in child online protection. To ensure a child-centric approach, 16 Focus Groups discussions were held with 113 children (49 boys and 64 girls) aged 13-17 in four research sites in five governorates (Grand Tunis , Tunis, Manouba), Jendouba, Gafsa, and Kasserine). To corroborate and contrast these findings, an additional seven focus groups were held with 28 parents and 22 educators. These qualitative research findings provide detailed accounts, personal perspectives, and valuable insights into the digital lives of children in Tunisia. This data provided detailed recommendations on the next steps towards ensuring that the collective rights of children in Tunisia are realized and a safe online environment is fostered.

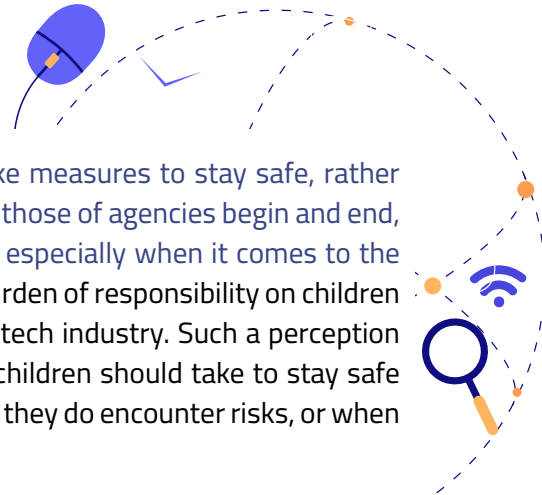
3. Research findings

The findings are categorized into three main topics: Internet Benefits and risks; Prevention and response to online risks and harms faced by children; and recommendations.

3.1. Internet benefits and risks


- 
- **In moderation, internet use provides many educational, social and economic benefits to children in Tunisia.** Focus group discussions with children revealed that Tunisian children are aware of and enjoy numerous educational and social benefits from using the internet. While parents and teachers' perceptions of benefits were largely limited to the educational and information benefits, children were far more aware of and likely to take advantage of a broader spectrum of opportunities, including entertainment, personal development, and commercial opportunities, in addition to providing mental health benefits. Specifically, children spoke of:
 - Educational benefits - how the internet can enhance their academic learning, improving language skills, improving general knowledge and learning new skills, and enhancing openness to other cultures.
 - Social benefits – such as maintaining and building social relations, entertainment, commercial and income generation, and
 - Mental health benefits, such as de-stressing. While the opportunities to de-stress online were presented as important benefits by children, children were also open about how this could in term, become problematic when taken too far, with some noting how being online could present an opportunity to “escape reality”, offering both an important, safe, and comfortable space for children to escape from pressures offline, but at the same time risking leading to social isolation and withdrawal if too much time was spent online.
- 

- 
- However, the research demonstrated children (and adults') awareness, and experiences, of how excessive internet use can equally have negative physical, social, and mental health impacts.
 - Both parents and children frequently mentioned excessive internet use, that could lead to social isolation, as well as distracting students from their studies. In some instances, excessive use was erroneously associated with autism, reflecting some of the common misconceptions and misinformation that permeate the discourse around excessive internet and device use.
 - Children also spoke of experiences of cyberbullying, at times emanating from and reinforcing regional and socio-economic divisions, but also inflicted through body-shaming. Bullying primarily occurred on Facebook but was also commonly experienced across other platforms such as Instagram and TikTok.
 - Both boys and girls spoke of online sexual harassment and other forms of sexual exploitation and abuse, often through unsolicited contact online, or non-consensual sharing or posting of images and videos (image-based abuse). Most commonly discussed by girls, when children were asked to complete a brief self-complete survey at the end of the focus groups, the majority of respondents, both boys and girls, reported unwanted sexual experience online.
 - Hacking and the use of fake Facebook profiles were highlighted as facilitators of bullying, sexual harassment, and extortion. Children demonstrated personal responsibility for their online activity but recognized that children and parents should have greater awareness about the risks the internet poses.
 - Importantly, children reflected a widespread awareness of the potential risks that exist online, particularly related to personal data and privacy, and participants discussed various measures they put in place to protect themselves. These included creating a secure Facebook account, withholding their real information on social media, including their real age and home address, not authorizing apps to access their data, not accepting people they don't know on social media, keeping their photos private, and reporting any suspicious profiles or content.
 - Despite this, children generally thought that they needed more information to develop their skills regarding protecting themselves and their data.
 - The research reveals the gendered nature of some internet benefits and risks. For instance, while boys are most likely to derive commercial and financial online benefits, girls are disproportionately affected by online sexual harassment and online extortion.
 - Additionally, a lack of awareness of legal safeguards and reporting mechanisms, coupled with societal norms, serves as barriers to reporting. Children spoke of social norms leading to victim blaming, with this norms representing a major hindrance to reporting image-based abuse and online sexual exploitation.
- 

- 
- Children consistently saw it as their own responsibility to take measures to stay safe, rather than understanding where their roles and responsibilities, and those of agencies begin and end, and where does the responsibility of other critical actors lies, especially when it comes to the app developers and social media companies. This places the burden of responsibility on children themselves, rather than on those providing services, and the tech industry. Such a perception is often exacerbated by an over-emphasis on the steps that children should take to stay safe online, and by blaming children for their online behaviour when they do encounter risks, or when those risks translate to harms.
 - Children, as well as adults, also recognized that some children were at greater risks of harm online, and of the greater vulnerability of some children to risks. This often revolved around an awareness of how offline factors, such as depression or low self-esteem, could increase the risk of some children experiencing harms. This awareness of the intersection between online and offline risks and vulnerabilities is critical and speaks to the underlying need to target appropriate prevention and response measures to those children most at risk, and to take into account offline vulnerabilities when designing interventions to promote online safety and wellbeing.



3.2. Prevention and response to online risks and harms

- This research revealed a number of existing mechanisms and positive examples in the prevention and response to online violence in Tunisia. These include existing awareness raising and resilience programs planned or undertaken by the Ministry of Education and the MFFES, through the Centre National de l'informatique pour l'Enfant (CNIPE), and through civil society and international NGOs efforts and funding.



In addition, this research revealed a number of initiatives taken by child protection and justice individual organizations to enhance the provision of tailored support to child victims and their families. For instance, some child and family judges have capitalized on their discretionary powers to provide ad hoc psycho-social support for children who have been victims of online radicalization or who engaged in online extortion.

- There are widespread recognition and commitment to building children's resilience to online risks and harms through cultivating "soft skills" or "life skills." This is a critical aspect of fostering resilience, as well as, the capacity and skills within children to successfully navigate the risks that they will inevitably encounter online. Importantly, this approach is increasingly being integrated into the formal education system.
- Notwithstanding these positive examples, a number of notable institutional and legal gaps were noted:
 - Notably, despite the majority of stakeholders interviewed estimating that the existing legal framework is adequate, a consensus emerged around an implementation gap and the need to update current response mechanisms to align with legal advancements. This was specifically in response to the changes brought about by law 58 of 2017 (on gender-based violence), law 61 of 2016 (on preventing and combatting human trafficking), and decree-law 54 from 2022 on cybercrimes.

- 
- While existing legislation (including those new changes cited above) do not yet reflect the full range and scope of online child sexual exploitation terms and definitions, as advocated by the CRC and global strategies, most key informants felt that the legislation, as it stands, is adequate and does not need to be updated. While it is acknowledged that legislative change takes time, there is also a risk that by allowing for prosecutorial discretion and interpretation and application of laws and terms that are not clearly defined in relation to, and specific to, the online environment, these may be applied inconsistently.
 - Notably, and due to the reliance on the jurisprudence, it is important to highlight the gap in the provision of specialized training for family and child judges on child protection.
 - In addition, a significant gap emerged in the provision of services for victims and, in particular, psychological support to children. The existing initiatives, such as the BEC and the CEC, have been practically abandoned due to the lack of psychological support staff.
 - Relatedly, effective prevention and response are hindered by a lack of knowledge and technical capacity amongst key stakeholders on reporting and handling of online child abuse material. This includes knowledge and understanding of the obligation to report different forms of online violence and OCSEA by teachers and education officials. This lack of awareness is exacerbated by the potential for retribution and reprisals by those teachers who do know and act on their obligation to report, with examples provided of threats made to teachers reporting cases to the police.
 - The lack of knowledge also related to the handling and management of cases of child sexual abuse material (CSAM) in a way that protects the victims from further harm, and ensures a coordinated approach between those making reports of CSAM, the protection system, law enforcement and the technology companies.
 - These gaps are further exacerbated by the lack of the integration of online violence into a formal integrated case management system, and it is noted that the current revision and development of the integrated child protection case management system provides an important opportunity to meaningfully address this gap.
 - Notwithstanding these gaps and bottlenecks, there is a clear commitment and concern from key stakeholders within and outside of government, to meaningfully tackle down online child sexual exploitation and other forms of abuse, which will provide a solid platform to initiate meaningful change, building on the existing work that has already been done.
- 

V. Recommendations

This report advances a set of recommendations, drawn from findings revealed in this research as well as international models and best practice examples.

Considering the importance, and lack of, systematic data and children-centric research on the benefits and risks associated with internet use, increased investment in research and data collection is highlighted as a pre-requisite in this report, ensuring that children's voices and experiences lay at the crux of the development of policies and programmes affecting them.

Specific recommendations advanced in this report are divided into 1) those related to policy and legislation, 2) those related to capacity building and systems strengthening, 3) prevention and response recommendations, and 4) cross-cutting institutional recommendations.

1. Policy and legislation

- Legislation should be reviewed and if necessary, amended, to ensure consistency across instruments and laws, as well as consistency with the most recent legislative guidance and knowledge. Consistency is required across legislation in order to ensure common standards by different actors within the protection, law enforcement and judicial response to online violence, and if possible to avoid judicial and prosecutorial discretion.
- A consistent and equitable enforcement of existing laws and policies must be applied, and accountability mechanisms formulated for when this is not the case.
- Prioritize the reform of the Child Protection Code, ensuring a victim-centric approach and ensuring recourse for victims who have experienced online child sexual abuse and exploitation, in line with the recommendations of the CRC and General Comment No 25.
- Establish Industry Guidelines on Child Online Protection, building on and domesticating the ITU Guidelines on Child Online Protection, and establishing a consistent and equitable enforcement of existing laws and policies must be applied, and accountability mechanisms formulated for when this is not the case.

1.1 Capacity-building and systems strengthening

- Reinforce capacity and provide training across stakeholders to ensure a consistent and equitable enforcement of existing laws and policies is applied, and accountability mechanisms formulated for when this is not the case. This includes training for:
 - Child protection workers (including auxiliary workers)
 - Teachers and education officials
 - Child justice and family judges

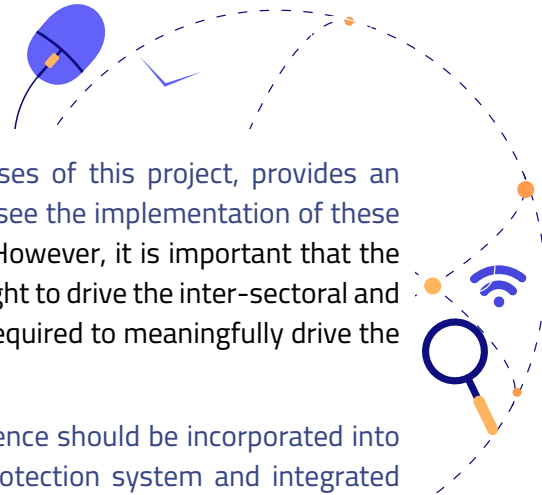
- Law enforcement and all those involved in reporting and handling reports of OCSEA, and in the handling of CSAM and related evidence. This may also entail training for those within the technology industry directly responsible for handling reports, preservation, and adhering to orders of CSAM.

1.2. Prevention and response mechanisms

- Invest in awareness-raising and social and behavioural change strategies that include online safety. These should include universal awareness programs, but also, more targeted social and behavioural change strategies targeting some of the known drivers and risk factors for online violence, including gender norms.
- Target awareness campaigns to break down taboos and obstacles to reporting extortion and sexual harassment, while reinforcing a culture of open and safe dialogue between parents and children.
- Parents and teachers must be made aware of the various opportunities and benefits that the internet offers to children, and the importance of the internet and digital technology to realizing the range of rights that children have. which has been shown to yield no positive outcomes and be ineffective.
- Provide targeted support for parents and caregivers, from birth through to adulthood. Evidence increasingly points to the importance of supporting parents and caregivers of very young children, in how to support their children adequately as they first start to engage with digital technology.
- Integrate basic digital literacy, digital parenting and safety skills into ECD Early childhood development and parenting programming. This can yield substantial benefits for both children and parents. Existing initiatives in partnership with the Tunisian government offer opportunities to integrate digital safety into existing programming with minimum additional investment , while offering a favourable cost-benefit outcome.
- Expand the reach of existing (sometimes nascent) government awareness initiatives such as Santé Globale programme and those offered by CNIPE .
- Enhance psycho-social support provision for children, through reinforcing the role of specialized civil society actors, through increased collaboration with the CPD, to fill the gap in psychological support provision. This must be undertaken through, others partnership agreements which compel civil society actors to maintain the confidentiality and anonymity of children, and to reactivate the BEC and the CEC.

1.3 Ensuring inter-government coordination on child online protection

- Child protection online should be integrated into all ministries involved in any activities with, or providing services to children, including Ministry of Education. In the case of education, this is particularly so as the Ministry pilots the use of tablets and ICT within schools. Global guidelines on the Child Online Protection and the use of EdTech provided by UNICEF can be a valuable starting point for this process.

- 
- The existing steering committee, established for the purposes of this project, provides an excellent starting point for a coordinating mechanism to oversee the implementation of these recommendations, as well as to support and drive the NAP. However, it is important that the COP working group established has the endorsement and weight to drive the inter-sectoral and inter-ministerial engagement and collaboration that will be required to meaningfully drive the National Action Plan on Child Online Protection.
 - Online risks and the identification and handling of online violence should be incorporated into the development and strengthening of the broader child protection system and integrated case management, currently under development. This can form the basis of strengthening the protection system to ensure readiness and capacity to adequately deal with those cases of sexual and other forms of online violence that require formal child protection intervention or management.

I. Introduction

This report analyses qualitative data gathered by Resolve Consulting and the Centre for Justice and Crime Prevention (CJCP) for the UNICEF-funded project “lutte contre la violence en ligne contre les enfants en Tunisie”, undertaken in partnership with the Ministère de la Famille, de la Femme, de l’enfance et des seniors (MFFES). The findings and recommendations detailed in this report will form the basis of a governmental and multi-stakeholder National Action Plan to prevent and respond to online violence against children in Tunisia.

1. Background

According to UNICEF’s The State of the World’s Children 2017,⁵ 1 in 3 internet users is a child and every day, more than 175,000 children go online for the first time.⁶ Information and communication technologies (ICTs) are central to children’s everyday lives in almost every part of the world. The use of ICTs has transformed the environment in which children grow and develop with online technologies now embedded in the everyday practices of young people in their communication, socializing and interactions with the world around them. This shift has been even further catalyzed by the response of many governments, including the Government of Tunisia, during the response to the COVID-19 pandemic, where children’s communication, education, and even play, shifted online at an unprecedented rate.

Even where children do not have access to digital technology themselves, they are likely impacted in some way by the use of technology by family members or by the world around them. Children have little or no choice in the way in which technology is part of their lives, and nor are they born with the inherent skills or knowledge to manage the risks that technology presents.

The world that children inhabit, therefore, is no longer clearly delineated by what occurs offline and what occurs online. To understand online violence, such as cyberbullying, online sexual exploitation, or image-based sexual abuse, as new forms of violence that occur online, it is necessary to examine the drivers and relationship between forms of violence that occur online and those that occur offline.⁷ Research on cyberbullying, for example, has shown that there is a strong relationship between children who bully online and those who bully offline.⁸ Also, the grooming of children, which may be initiated online, may then move offline or remain online through live streaming or other forms of abuse.⁹ The intersection between online and offline violence is also reflected by the growing body of evidence on how best to prevent and respond to both online and offline violence. This includes the conceptualization and evidence base on what works in intervening and preventing violence both online and offline.

5 State of the World’s Children 2017: Children in a Digital World. UNICEF, New York. <https://www.unicef.org/sowc2017/>

6 Safer Internet Day Press Release. UNICEF, New York, 6 February 2018. https://www.unicef.org/media/media_102560.html

7 Kardefelt-Winther, D., Maternowska, C. (2020) Addressing violence against children online and offline. *Natural Human Behaviour* 4, 227–230. <https://doi.org/10.1038/s41562-019-0791-3>

8 Haddon, L., and Livingstone, S. (2014) The relationship between offline and online risks. *Young people, media and health: risks and rights: Nordicom Clearinghouse Yearbook 2014* (pp.21–32). Eds. C. von Feilitzen and J. Stenersen. Goteborg: Nordicom.

9 UNICEF East Asia and the Pacific Regional Office, What Works to Prevent Online and Offline Child Sexual Exploitation and Abuse? Review of national education strategies in East Asia and the Pacific, UNICEF, Bangkok, 2020.

Importantly, there is a risk that the discourse on online risks and harms will lead to the marginalization of the rights and opportunities to access and use the internet in the name of safety. Internet risks and opportunities are not dichotomous¹⁰. Therefore, understanding children’s online experiences, both the negative and the positive, are best understood within a child rights and protection framework. This has been emphasized through the publication of the recent General Comment No: 25 of the UN Committee on the Rights of the Child (CRC), which argues that all rights of the child as recorded offline, exist within the digital space, and notes that:

“The rights of the child must be respected protected and fulfilled in the digital environment. Innovations in digital technologies affect children’s lives and their rights in ways that are wide-ranging and inter-dependent, even where children themselves do not have access to the internet. Meaningful access to digital technologies can support children to realise their full range of civil, political, cultural, economic and social rights.” (Article 4, GC No. 25 of 2021 on Children’s Rights in the Digital Age.)

The General Comment further builds on Article 12 of the Convention on the Rights of the Child which notes that:

“State parties identify and address the emerging risks that children face in diverse contexts, including by listening to their views on the nature of the particular risks that they face” (General Comment No. 25 III.C.14.)

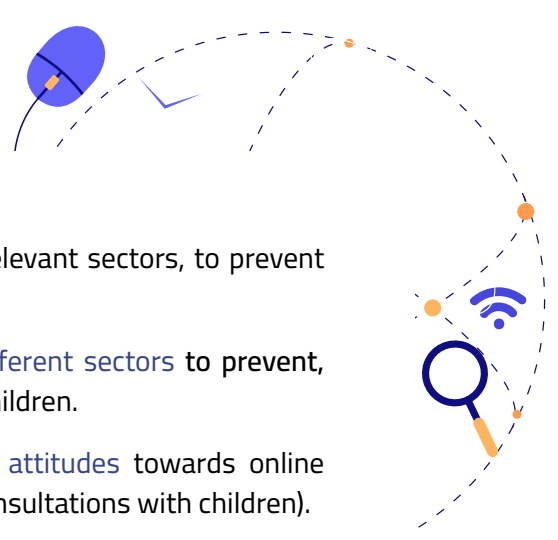
Additionally, it is important to note that the risks posed by technology to children may impact children who do not have access to this technology themselves. The conditioning of children for sexual exploitation (grooming) can happen offline and then move to the virtual space. Cyberbullying can occur by others using mobile devices or other forms of technology while involving victims who themselves do not have direct access to that technology. In addition, many of the skills and protective factors that children need to improve their safety online are common to those that serve as protective factors offline. Strategies on keeping children safe need to take into account how to foster skills and how to promote resilience, both offline and online. It is important that in all aspects of any policy or strategy to keep children safe online (and offline), the needs, vulnerabilities and protective factors of children are fully considered.

2. Study objectives

This project aims to support the Tunisian government, through the PPIPPE and UNICEF’s Country Programme 2021-2025, in strengthening the national capacity to prevent, detect and respond to violence against children, including through social workers, multisectoral coordination, and changing social norms and behaviours on violence against children.

In particular, the project aims to support the MFES to strengthen the capacity of different sectors to address different types of vulnerabilities and violence against children in the virtual world.

¹⁰ binary and dichotomous are synonyms.



This will be achieved through:

1. Mapping the current legislative and policy context, in all relevant sectors, to prevent and combat online violence against children .¹¹
2. An assessment of the current needs and capacities of different sectors to prevent, respond to and support victims of online violence against children.
3. An exploration of children's experiences, knowledge and attitudes towards online violence and help-seeking behaviours (collected through consultations with children).

This will lead to the development of a National Action Plan (NAP) to combat online violence against children in Tunisia.

The study will answer a series of questions:

- To what extent are protection against online violence (exploitation, violence and abuse of children online) and the promotion of online safety in all its forms integrated into legislation and policy in Tunisia?
- To what extent are different sectors within government, civil society and industry aware of their roles and responsibilities, and able to prevent and respond to online violence against children?
- What structural and organizational measures and coordination mechanisms exist to ensure an intersectoral response to the prevention of online violence against children in Tunisia (intergovernmental and societal)?
- In the absence of national or subnational data, what are children's online experiences and knowledge and capacities regarding their rights and protection online, in line with CRC General Comment No. 25?
- What are the barriers that exist for a cross-sectoral response to and in preventing and responding to online violence against children in Tunisia, and how can they be addressed given the existing constraints that could be encountered?




3. Research Methodology

The review of conceptual literature and international conventions that Tunisia has ratified (Annex 1), along with the mapping of the Tunisian legal and institutional framework for child and online protection (Annex 2) has facilitated the design of a research methodology suitable for collecting data to support the development of a national action plan. The research design and methodology, including a complete research protocol which includes all interview guidelines and Focus Group questions, were shared with UNICEF Tunisia and the MEFFS for approval. In addition, the team submitted the research methodology and protocol for ethical assessment and review by HML Institutional Review Board (IRB).¹²

¹¹ While this note refers to online violence against children, the intersection between online and offline violence will be explicitly recognized throughout this proposed work.


¹² HML Institutional Review Board <https://www.healthmedialabirb.com/>




This study's human subjects' protection protocols received HML IRB ethics review approval on July 26, 2022 (approval number #592TUNI22).

Due to 1) the intersection of online and offline violence, and 2) the common drivers of online and offline violence, abuse and exploitation, the research approach seeks to understand this violence with both prevention and response perspectives in mind. Therefore, an analysis of existing risks and protective factors, across the different domains in which children live – individual, family, relationships, community, and macro or micro-societal – must be captured. The Global Kids Online research methodology emphasizes the need to interrogate factors across all sectors that may influence a child's life and development, from health to education to justice to telecommunications. Therefore, the inclusion of perspectives from individuals with expertise and professional experience in these fields, in addition to policy-makers, child protection officers and service providers is valuable. Health and education professionals provide an important interface with children, particularly concerning help-seeking behaviours, and directly addressing harms that may result from adverse online experiences. Justice professionals highlight how the laws are being implemented and whether decisions are being made with the children's best interests at heart. Technology industry representatives address how these companies provide support or respond to protection issues. Furthermore, capturing children's perspectives of the status-quo, the challenges and experiences, and the existing prevention and response mechanisms assesses the range of issues that need to be addressed and ensures that the national action plan includes child-centric perspectives. This has facilitated an assessment in this report of existing capacities, gaps and direction that can be explored in relation to the global frameworks for country-level response to online violence, including the Model National Response (MNR) developed by the WeProtect Global Alliance. The MNR provides a cross-sectoral approach to preventing and responding to online violence against children and identifies the roles of different sectors of government and society.

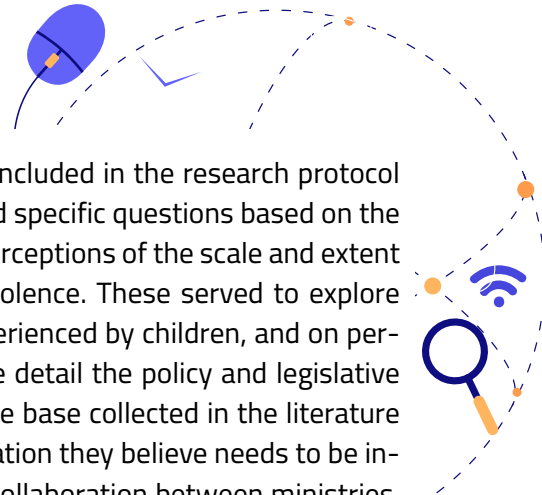
In addition to the desktop review, the study collected qualitative data from children and key stakeholders involved in all aspects of child online protection. This data collection entailed:

- 
- key Stakeholder Interviews with child protection and telecommunications actors
 - three sets of Focus Groups with:
 - Children (including an anonymized self-completion survey)
 - Teachers and education professionals
 - Parents

4. Key Stakeholder Interviews




The Key Stakeholder Interview (KSI) is an effective and efficient qualitative research method that allows researchers to gain insights from stakeholders who are especially well-informed about the field and will be directly impacted by the policy recommendations. In-depth KSIs were conducted with experts and informants who possess relevant knowledge and experience in Child Protection, education, and prevention and response to (online) violence. Interviewees included key stakeholders within the various government ministries, the legal system, the education system, regulatory structures, and civil society groups working on child protection and violence prevention.

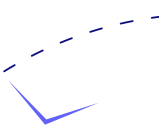


The research team designed a semi-structured interview guide (included in the research protocol in Annex 3) which included a set of questions for all interviews and specific questions based on the interviewee's profession. The interviews explored respondents' perceptions of the scale and extent of the problem and perceived challenges to addressing online violence. These served to explore stakeholders' perceptions and knowledge of risks and harms experienced by children, and on perceived roles and responsibilities. The interviews explored in more detail the policy and legislative environment and implementation gaps, building on the knowledge base collected in the literature review and legal and institutional mapping, and asked what legislation they believe needs to be introduced or better implemented. Furthermore, coordination and collaboration between ministries, as well as between government, industry and civil society were explored in detail. After an initial contact list was shared by the MFFES – the project's lead agency – the project followed a snowball sampling approach. 17 formal interviews and meetings were undertaken as part of this research (please see Annex 4 for a list of interviewees).

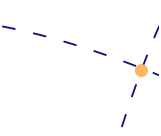
5. Focus Group Discussions



Focus group discussions provide an important opportunity to test particular understandings, experiences and messaging around internet usage and safety. This qualitative research method enables the collection of in-depth data that provides more details about the phenomenon under study than broad survey questionnaires.¹³ Furthermore, focus groups are the most suitable method for this study for the following reasons. first bullet point, as there is a lack of child-centric data from Tunisia on children's internet experience, focus groups are ideal for "an in-depth exploration of a topic about which little is known."¹⁴ This is especially important because although the focus group design and activities are based on previous studies and issues the research aims to explore, "focus groups have the potential to generate unexpected and unpredictable outcomes both in terms of the data collected and the complexities of the research process as a whole."¹⁵ This ensures the research both deductively tests research assumptions and inductively enables the participants to influence the trajectory of the research, and ultimately of the National Action Plan.



second bullet point, focus groups is an ethically responsible method for conducting research with minors. This is because FGs can help "create a safe peer environment for children"¹⁶ and redress the "power imbalances between researchers and participants" that would exist in a one-on-one interview between an adult and a child.¹⁷



third bullet point, it is an inclusive method because it is suitable for people with disabilities, such as visual or communication impairments or people who have problems with writing or reading.¹⁸, and vulnerable people. Fourthly, similar qualitative studies on children's online experience in other countries use focus groups, often in addition to individual interviews.

13 Barbour, R. S. (1999). The use of focus groups to define patient needs. *Journal of Pediatric Gastroenterology and Nutrition*, 28, S19–22

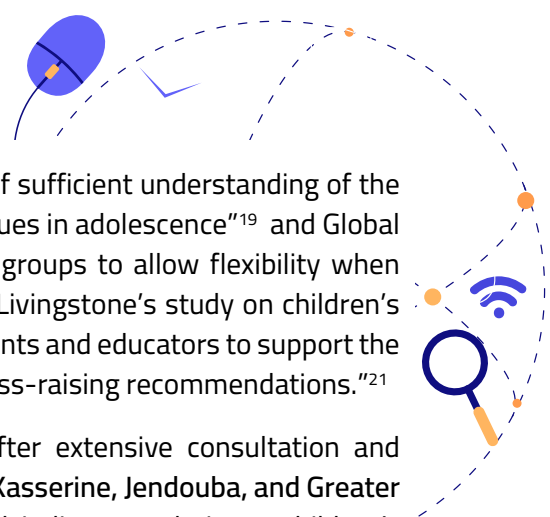
14 Stewart and Shamdasani (1990) p. 102

15 Parker and Tritter (2006) p.34.

16 Adler, K., Salanterä, S., & Zumstein-Shaha, M. (2019). Focus Group Interviews in Child, Youth, and Parent Research: An Integrative Literature Review. *International Journal of Qualitative Methods*, 18. p.2

17 Shaw, C., Brady, L.-M., & Davey, C. (2011). Guidelines for research with children and young people. NCB Research Centre. London, England: National Children's Bureau. p.4

18 Adler, K., Salanterä, S., & Zumstein-Shaha, M. (2019). Focus Group Interviews in Child, Youth, and Parent Research: An Integrative Literature Review. *International Journal of Qualitative Methods*, 18. p.1




Stoilova et al (2019) used “focus groups because there is a lack of sufficient understanding of the relationship between digital technology use and mental health issues in adolescence”¹⁹ and Global Kids Online (2016) designed a framework which included focus groups to allow flexibility when seeking to “understand[...] children’s rights in the digital age.”²⁰ Livingstone’s study on children’s data and privacy online conducted focus groups with children, parents and educators to support the development of “child-inclusive policies and educational/awareness-raising recommendations.”²¹

The location of each of the research sites was determined after extensive consultation and discussion with the MFFES.²² The focus group locations of Gafsa, Kasserine, Jendouba, and Greater Tunis were selected based on three important, and interconnected, indicators relating to children’s vulnerability established in consultation with the MFFES : regional development indicators, Baccalaureate success rate, and school dropout rate.²³ This ensured that the focus groups respond to research needs while accounting for budget and timeline limitations.

5.1. Focus Groups with children

The research team organized 16 FGs with 113 children between the ages of 13 and 17, including 64 girls and 49 boys from four research sites in Tunisia: Grand Tunis (Manouba, Tunis), Kasserine, Gafsa, and Jendouba. The focus groups with children aimed to understand how children in Tunisia use the internet, for what purposes, if they take risks, and if they have been exposed to harms. Please see annex 3 for a detailed discussion of the indicators used to select the research site in consultation with the MFFES and the steering committee. The sample in each site ensured an equitable gender and age distribution. In each of the four selected sites, the team conducted three focus groups: boys only, girls only, and a mixed boy/girl. While the FG facilitator endeavored to create a safe space for all discussions, the inclusion of a girls-only group ensured a safe and comfortable space to openly discuss their experiences and knowledge. This is important because gender differences might arise in groups of teenagers or discussions of gender-specific topics.²⁴



Consequently, we hypothesized that the different gender compositions of the groups would yield different outcomes, thus leading to a more comprehensive dataset. The gender of the focus group moderator can also influence data collection,²⁵ so while a male moderator facilitated some of the mixed groups, all girls’ groups were facilitated by a female moderator.

In addition, to ensure the diversification of children respondents and the inclusion of vulnerable children, the research team coordinated with the Centre Intégré de la Jeunesse et de l’Enfance Cité el Khadra to organize three focus groups.

19 Stoilova, M., Edwards, C., Kostyrka-Allchorne, K., Livingstone, S., & Sonuga-Barke, E. (2021) Adolescents’ mental health vulnerabilities and the experience and impact of digital technologies: A multimethod pilot study. London School of Economics and Political Science and King’s College London. p.79

20 Stoilova, M., Livingstone, S., & Kardefelt-Winther, D. (2016). Global Kids Online: Researching children’s rights globally in the digital age. *Global Studies of Childhood*, 6(4), p.460.

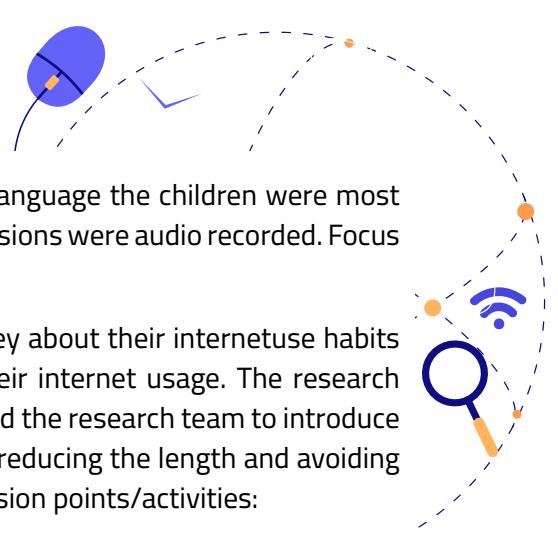
21 Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children’s data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science.

22 Project meeting August 29 2022

23 The relevance and application of these indicators to site selection is explored in more detail in Annex 1.

24 Fielden, A. L., Sillence, E., & Little, L. (2011). Children’s understandings’ of obesity, a thematic analysis. *International Journal of Qualitative Studies on Health and Well-Being*, 6. doi:10.3402/qhw.v6i3.7170

25 Adler, K., Salantera, S., & Zumstein-Shaha, M. (2019). Focus Group Interviews in Child, Youth, and Parent Research: An Integrative Literature Review. *International Journal of Qualitative Methods*, 18. p.4



FG discussions were conducted in Tunisian dialect, which is the language the children were most comfortable speaking. With the participants' permission, FG discussions were audio recorded. Focus groups ranged between 4 and 13 participants each.

At the start of each FG, children were provided with a short survey about their internet use habits and frequency. This aimed to allow participants to reflect on their internet usage. The research protocol was tested on a pilot focus group of 6 participants. This led the research team to introduce several modifications to the initial research methodology, mainly reducing the length and avoiding repetition. The FGs with children were based on four broad discussion points/activities:

- **Introduction:** including what applications/social media platforms they use the most and what are their main reasons for using the internet;
- **Benefits and risks:** on post-it notes, participants respectively wrote the benefits and risks (one per post-it) related to the use of the internet/social media. Using a flip chart, with a horizontal line dividing the paper in two with a happy face drawn on the left and a sad face on the right, participants put their post-it notes on the appropriate side. The benefits were discussed at length first before moving to the risks;
- **Data protection:** participants discussed what the internet knows about them and what measures do they take to protect their personal data and their safety;
- **A better internet:** participants were invited to discuss the improvements they wish to see introduced to the internet to improve their safety.

At the end of each FG, children completed an anonymous 19-item self-report questionnaire to address more sensitive questions about children's negative experiences online. This included an open-ended question about experiences that they may not feel comfortable disclosing in front of peers.

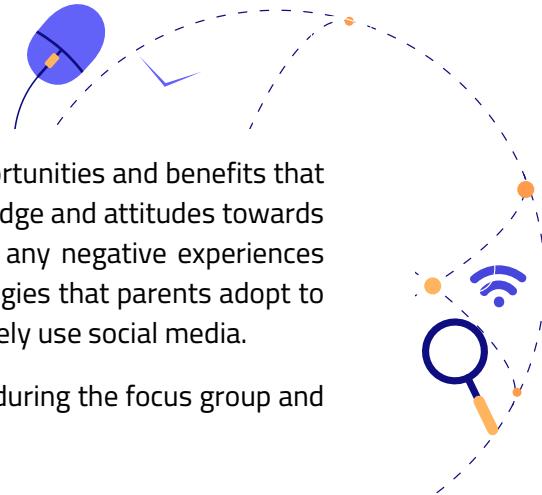


5.2. Focus Groups with parents

The research team organized four (4) FGs with 28 parents. The FGs with parents aimed to explore what are the parents' concerns in relation to children's social media usage and experiences, and how this aligns with children's experiences. These FGs sought to explore parents' understanding and knowledge of their children's social media and digital technology use, in addition to the strategies they employ to manage the associated risks while maximizing the benefits.

The FGs with parents were based on three discussion points/activities:

- **Introduction:** including how they use social media and what they enjoy the most about social media.
- **Managing children's internet use:** exploring parents' understanding and knowledge of their children's social media and digital technology and the management strategies they employ.



This discussion aimed to explore parents' views of the opportunities and benefits that social media provides for their children and parents' knowledge and attitudes towards their children's social media use. It also aimed to discuss any negative experiences their children may have encountered and explore the strategies that parents adopt to mediate these online risks and ensure their children can safely use social media.


- **Discussion summary:** clarifying the main points discussed during the focus group and emphasizing the positive shared aspects.

5.3. Focus Groups with educators

The research team organized three (3) FGs with 22 educators. The FGs with teachers aimed to speak to people who educate or provide support to children, such as teachers, school counsellors, and social workers, on their perceptions and experiences of children's activities and experiences on social media. The FGs with educators followed a similar structure as FGs with parents.


6. Ethics and child protection

As mentioned above, protocols for the protection of human subjects in this research were assessed through a research ethics review by HML Institutional Review Board (IRB) and received ethics approval on 26 July 2022 (approval number #592TUNI22).



In addition to ensuring the research design aligned with research ethical guidelines for the protection of human subjects, special attention was placed by the research team on the safety and confidentiality of children focus groups. Due to the potential sensitivity of the subject matter, respondent confidentiality is vital. Therefore, at the outset of each children FG, participants were invited to choose an alias/fake name to be used in the report write-up. Therefore, the names of children appearing in quotes in this report are all aliases chosen by the children themselves. At the end of the self-completion survey, the following confidential help was offered to the youth participants.

"Is something you've spoken about today bothering you? Remember, you can talk to the facilitator after you are done here, and he or she can help you find someone to talk to in private and anonymously!"



The research team and partners from the MFFES developed a referral protocol to ensure that any child who disclosed abuse, or needed protection or referral, received the required support. A referral mechanism directly to the national Helpline and ministry was established. The team worked closely with the child protection team within the Ministry to ensure that this occurred. Two children participating in a female only focus groups requested confidential psychological support. The research team coordinated with UNICEF and the MFFES and identified a ministry-affiliated psychologist in their area. We are pursuing the coordination with the two children to ensure they are receiving the necessary psychological follow-up. Due to the lack of capacity and reach of child protection system, future research should consider addressing solutions to this issue.

7. Data analysis

Focus group and interview data underwent deductive and inductive analysis through qualitative analysis software NVIVO 12. In the first level of analysis, the research team coded the data into pre-determined deductive codes: Benefits of internet use, risks and harms associated with internet use, existing measures and policies, existing gaps, and recommendations. Findings under each of the benefits and risks codes are elaborated in detail under each sub-section of the Research Findings section of this report. Findings under the codes of existing measures and policies, and existing gaps, are discussed under Section 3. As a second step in the analysis, data under each code was further analyzed, and the research team extracted inductive sub-codes for each code. In some instances, sub-codes were divided into further sub-codes.

In addition, data from the children focus group pre-survey and the anonymous questionnaire was input into excel and trends were revealed through the use of advanced excel quantitative analysis tools.

8. Methodology limitations

This research adopts a qualitative methodology which aims to produce in-depth and child-centric data including detailed description of personal accounts and experiences. The research does not claim to be representative of Tunisian youth and a broader study, and FGs in other governorates would have produced a larger data set from which to draw more certain conclusions. For example, the inclusion of other high child vulnerability governorates, such as Kairouan, in addition to lower child vulnerability governorates, such as Sfax, would have produced greater diversity of responses. Notwithstanding the case selection of governorates, based on the intersection of three relevant indicators, relating to child violence, and the range of youth participants, ensures the collected data is both specific to individual cases and indicative of a broader, national context. Thus, the results can be considered generalizable since the 16 FGs produced similar responses in the 'benefits' (social, educational) and 'risks & harms' (bullying, harassment, fake profiles and extortion) categories. However, the research did not include the perspectives of minority groups, namely children with disabilities and migrant or refugee children.

While Focus Groups were selected to ensure child safety and female only groups allowed participants to be more candid with their responses, it is possible that due to the sensitivity of the subject matter, some participants may not have felt sufficiently comfortable sharing all the negative online experiences. Despite the ensured confidentiality, some participants knew each other and may not have been willing to share embarrassing examples. Validity was ensured by using Tunisian nationals as moderators who followed the four part FG structure and were able to collect low inference qualitative explanations of children's online experiences. Furthermore, the rigorous coding process ensured the emergence of patterns in the data.

Regarding the collected survey data from the self-reporting questionnaire, the small sample size in relation to the national population makes this unrepresentative data. However, the questionnaire provided an opportunity, through an open-ended question, for children to safely and anonymously share sensitive or upsetting experiences that they may not have felt comfortable sharing in the FG setting. Also, the survey provides an indication of interaction with, exposure to, or generation of, sexual content, texts or other disturbing material that may not have been addressed in the FG discussions.

II. Internet benefits and risks: A child-centric perspective

In order to promote a children-centric understanding of children's positive and negative experiences online, analysis and coding of children focus group data centred on revealing the perspectives and experiences of children regarding the benefits of and risks and harms associated with internet use. These are respectively outlined in the following two subsections. Where relevant, analysis of data from children focus groups is juxtaposed with findings from parents and educators focus groups, highlighting the gaps that exist in understanding children's experiences with the internet and its impact.

1. In moderation, internet use provides many educational, social, and economic benefits


Focus group discussions with teachers and parents revealed an initial reluctance on their part to acknowledge and discuss the positive impacts that internet use has on children's lives. When prompted and probed by the facilitator to hold a discussion about perceived benefits, the discussions were often largely limited to educational benefits and easy access to information. These were discussed in broad terms, revealing a general lack of parental and educational staff engagement with the specific online tools and sources used by children to enhance their educational experience and access information.

The children FGs corroborated the parents' and teachers' perceptions about the internet's educational benefits. However, discussions with children produced much richer data and findings around the specific tools and measures they utilized to advance and complement their school-based learning through the internet. Furthermore, analysis of children FGs revealed an array of other benefits across all areas of their lives, which have not been mentioned by, or are not known to, their parents and educators.

2. Educational benefits

2.1. Enhancing academic learning

Children reported several educational benefits from internet use, with the majority using google and educational websites (such as TakiAcademy) to conduct research and enhance their understanding of their lessons or understand homework. YouTube was also noted as an important website for learning or helping with homework across focus groups. In particular, FG8 mentioned YouTube channels dedicated to explaining school material. It is worth noting that this benefit was caveated in some FGs, and discussions signaled the limits of the use of the internet to enhance academic learning-related learning. For instance, in FG7, participants agreed that, while using the internet to complete homework may be useful, some students may abuse this tool, instead blindly copying entire lessons and research assignments without absorbing the information.



This was highlighted in an interview with Ms. Najet Souli, a senior emeritus professor, who complained that “nowadays if a child has an assignment to research a plant or the different kinds of herbivorous and carnivorous animals, they will go to the internet café and ask them to retrieve a whole research paper for 2 TND. 90% of the information won’t stick” (interview with researcher).

Improving language skills:

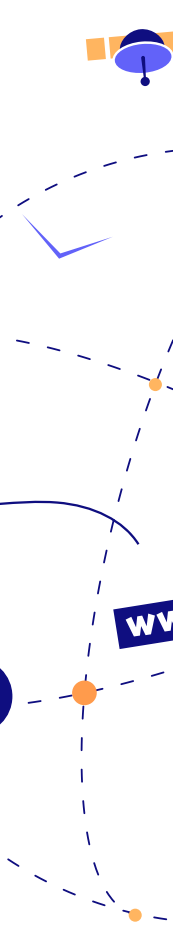
The majority of children reported benefits related to language learning through translation apps, language learning tools like Simply, Duolingo, Google Translate, and Memrize, watching foreign language content, or communicating on social media and through online gaming.

Improving general knowledge and skills:

Many children reported using the internet to keep abreast of the news, follow topics of their interest, and learn new skills while honing existing ones (painting, cooking, chess, photography, video production and editing, design, dance, and make-up).

Enhancing understanding of and openness to different cultures:

Whether through making online friends from different countries and cultural backgrounds or through watching series and movies, the majority of children reported an improved understanding of different cultures and appreciation for diversity. This benefit was especially highlighted amongst participants from rural areas and interior regions, arguably due to their socio-economic marginalization which limits their movement and their opportunities to meet diverse people in person. Indeed, as one participant from the rural Manouba region of Tebourba stated, “the internet introduces me to new things I would’ve never encountered in real life otherwise” (Zarga, 17, male). FG6 participants also reported expanding their horizons through forging new friendships from across the world. This reflects findings from other countries, where children view the internet as the only way of expanding their world, and where meeting new friends online, from other cultures and regions, is one of the major drawcards of being online.²⁶



ONE OF THE ADVANTAGES TO BEING ONLINE, FOR MANY CHILDREN IN TUNISIA, WAS MEETING OTHERS FROM DIFFERENT REGIONS OF THE WORLD, AND FROM OTHER CULTURES. THIS IS PARTICULARLY IMPORTANT FOR THOSE LIVING IN RURAL, OR OFTEN MARGINALIZED, COMMUNITIES. YET THIS ALSO REFLECTS ONE OF THE TENSIONS APPARENT IN COMMON APPROACHES TO INTERNET SAFETY. ONE OF THE CORE MESSAGES OF MANY ONLINE SAFETY CAMPAIGNS, AND ONE PRIORITIZED BY MANY PARENTS AND TEACHERS, IS THE IDEA OF “STRANGER DANGER”, AND CHILDREN ARE DISCOURAGED FROM TALKING TO STRANGERS ONLINE. YET, THE MAJORITY OF SEXUAL RISKS CHILDREN ENCOUNTER COME FROM THOSE KNOWN TO THEM, RATHER THAN STRANGERS (WHO, 2022). THIS IS JUST ONE EXAMPLE OF HOW MESSAGING THAT HAS NO FOUNDATION IN EVIDENCE, CAN INHIBIT ONE OF THE MAJOR ADVANTAGES AND BENEFITS FOR CHILDREN, RATHER THAN EQUIPPING THEM WITH THE SKILLS TO MANAGE THE INTERACTIONS THAT DO HAVE ONLINE, IN A SAFE AND INFORMED MANNER.

²⁶ Burton, P., Leoschut, L. & Phyfer, J. (2016). South African Kids Online: A glimpse into children’s internet use and online activities. Cape Town: The Centre for Justice and Crime Prevention.

2.3. Social benefits: Maintaining and building social relations:

Most participants use social media primarily to keep in touch with friends and family, with the majority reporting actively or organically making new connections and developing friendships online. This provided social and emotional benefits by enabling children to feel connected and develop a sense of belonging. This is consistent with findings from the Global Kids Online study across 11 countries, which shows that social media and chat platforms have become a crucial meeting place where children can meet and socialize with friends and family.²⁷

2.4. Entertainment

Participants listed the numerous ways in which the internet provides a source of entertainment. This included passive activities such as listening to music, watching videos, watching series and movies, and watching sport. Also, interactive forms of entertainment such as doing workouts/exercises, learning dance routines, gaming, and seeking inspiration for art and fashion were cited. Watching content (memes and videos) by social media influencers in addition to creating, editing and posting their own social media content were also frequently mentioned. That these children actively engage in creating, editing and interacting with memes and other content points to the fact that there is some level of creative technical skills applied on a regular basis, thus reflecting both the opportunity for entertainment and expression of some level of creativity, as well as skills beyond simply media consumption.

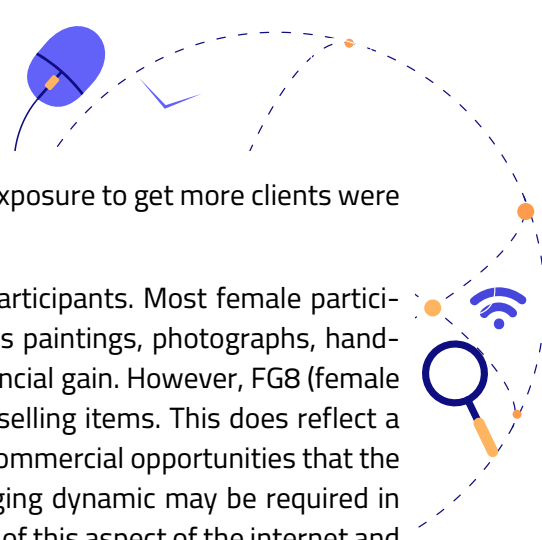
FG10 participants agreed that the internet keeps them safe at home and away from all the problems they can encounter outdoors. As one participant stated, “there is nothing good outdoors in Kasserine, only problems” (John, 17). Participants explained that they lack any means of entertainment and that “before we used to at least go to the Maison de Jeunes for free. Now, if you want to go to the Maison de Jeunes, you have to pay 5 dinars per day” (John, 17).

In addition, as Kortli explained, “each neighborhood in Kasserine is controlled by a group of boys, who will beat you up if you come to their territory” (17, FG10). **The internet provides a practical way for these children to escape physical harm and play in a safe space.**

2.5. Commercial benefits and monetary gain

A number of participants reported how the internet has helped to develop their professional and entrepreneurial skills. This has subsequently facilitated their businesses, enabling them to receive direct or indirect financial benefits from their internet use. Some participants learned and developed skills (photography, coding and app development) online and launched freelance careers monetizing their skills. As a house painter, and despite his part-time job not requiring the internet, Pastis (17, male), reported his business benefiting and garnering new clients from the exposure that social media provides him. Other participants made money from gaming, such as Jako (17, male) who collects and sells diamonds on the popular game Free Fire.

²⁷ Kardefelt Winther, Daniel; Livingstone, Sonia; Saeed, Mariam (2019). Growing up in a connected world, Innocenti Research Report, UNICEF Office of Research - Innocenti, Florence. Pg. 16. <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>




Receiving advertising money from making videos and increasing exposure to get more clients were also mentioned as financial benefits.

Notably, online entrepreneurialism was largely limited to male participants. Most female participants who use social media to post about their products (such as paintings, photographs, hand-made jewelry), do so without the intent of selling or making a financial gain. However, FG8 (female only) participants agreed that the internet facilitates buying and selling items. This does reflect a potential gender divide in how children are utilizing the potential commercial opportunities that the internet offers for children. A better understanding of this emerging dynamic may be required in order to ensure that both boys and girls are able to make the most of this aspect of the internet and digital connectivity.

2.6. Mental Health benefits

Participants mentioned the various ways in which the internet provides means to improve their mental health. FG5 participants discussed how watching entertaining videos helps them de-stress. Participants from the integrated center (FG2) cited passing time and “withdrawing from reality” as a benefit of social media, perhaps suggesting the difficult social reality of these institutionalized children and their finding solace in social media. FG4 participants also mentioned how the internet allowed them to “escape reality.”

Several FGs discussed the advantages of various support groups, enabling people to help each other and offer advice. Such groups connect people in need of help with others willing and able to provide this help. FG5 participants mentioned that receiving “likes” on pictures of themselves increased their self-esteem and that they found some mental health benefits from posting about difficult times they were experiencing. FG6 reported that keeping in touch with friends and making new friendships improved their self-esteem and sense of belonging.



The complexity of digital technology and internet use and mental health are often over-simplified, reduced to the more negative consequences of excessive internet use and exposure to “triggering” content, often algorithmically curated.²⁸ Yet, as evidenced in this research, the internet can often be a refuge or offer a safe space, where children can find support, and escape from difficult situations offline. The degree to which children can maximise the benefits, particularly those experiencing mental health difficulties, can often depend on their digital skills, and how they apply these, and so supporting children in developing these skills becomes even more important.²⁹

28 Vuorre, M., Orben, A., & Przybylski, A. K. (2021). There Is No Evidence That Associations Between Adolescents’ Digital Technology Engagement and Mental Health Problems Have Increased. *Clinical Psychological Science*, 9(5), 823–835. <https://doi.org/10.1177/2167702621994549>

29 Livingstone, S., Stoilova, M., Stănicke, L. I., Jessen, R. S., Graham, R., Staksrud, E., & Jensen, T. K. (2022). Young people experiencing internet-related mental health difficulties: The benefits and risks of digital skills. An empirical study. KU Leuven, ySKILLS.

3. Internet use is associated with new and enhanced physical, mental, and psychological risks and harms

While the benefits of moderate internet use are abundant, the focus group and interview research revealed significant online harms and risks. Thematic analysis of FGs data produced the following “risks and harms” sub-codes.

3.1. Excessive Internet use

The majority of participants highlighted the adverse effects of prolonged internet use on their physical health. These include eyesight problems, back pain and poor posture, spinal problems, weight gain, and headaches, in addition to concentration problems and memory loss.

Furthermore, “addiction” (the term “iidman” used by participants) was cited as a key risk across children, teachers, and parents focus groups. Participants defined internet addiction as excessive use of and/or dependence on the internet leading to negative impacts on social relations, cognitive function, educational attainment, and physical health. There was a general agreement that, while using the internet in moderation unlocks an array of benefits for users, internet addiction can isolate users from their family and friends. While the majority of participants agree that social media allows them to stay in touch with their friends and families, they equally cited the role of social media and the internet in causing isolation and eroding in-person connections amongst friends and family. The impact on some families and children can be devastating. As a participant from a center for children without family support explained, “my mother started using this app through which she met and chatted with people from all over the world. She became so addicted to it and withdrew from me and my siblings until it became child neglect, and we were taken away from her” (Yasmine, 14, female).

My mother started using this app where she met and chatted with people from all over the world. She became addicted to it and withdrew from me and my siblings until it became child neglect, and we were taken away from her” (Yasmin, 14).

Participants also thought that excessive use and addiction can also distract children from their studies while stunting mental and social growth and self-care. In addition, participants linked excessive internet use with poor concentration and psychological issues. While FG4 participants cited the internet allowing them to “escape reality” as a benefit, they also indicated that it can become unhealthy, stating that some people even undergo personality changes due to their isolation and their addiction to the internet. Participants noted that the internet can facilitate excessive use of, or addiction to, gaming, and watching shows, or pornographic material. They also noted this posed financial risks, such as spending too much money on online gaming.

This research highlighted a widely-held misconception that excessive use of the internet causes autism. In all children and parents FG that discussed autism, participants erroneously linked internet addiction to the onset of autism spectrum disorder (ASD). ASD is a biological disorder of brain development that is most probably caused by a combination of a child’s genetics and environmental factors during pregnancy.³⁰

³⁰ Altevogt, B. M., Hanson, S. L., & Leshner, A. I. (2008). Autism and the Environment: Challenges and Opportunities for Research. *Pediatrics*. 121(6), 1225–1229. doi:10.1542/peds.2007-3000.

This means that it cannot be caused, by any factor, in children. The origin of the general perception - that excessive internet, or screen time, causes autism - may be because people with autism tend to use the internet more as they find person-to-person interactions more challenging^{31,32}.

For example, "autistic adolescents spend more time online gaming than neurotypical peers."³³

Furthermore, screen time acts like a stimulant and excessive screen time may exacerbate symptoms since children with ASD are "uniquely vulnerable to various brain-related impacts of screen time."³⁴

3.2. Bullying

Findings from children FGs corroborate literature outlining the various forms that online bullying takes, including verbal abuse, hate speech, mockery disguised as banter, sexism, homophobia, colorism, ableism, and body shaming. The psychological impact on victims is severe. Participants from rural and interior regions expressed their vulnerability to online abuse by people from the coast or the capital whom participants perceived to look down upon them and call them derogatory names due to their regions, skin color, and accents. Bullying that perpetuates regional and socio-economic divisions, feelings of marginalization and being the subject of contempt were expressly discussed by FG participants in Tebourba, Gafsa and Kasserine. Kortli (17, male) noted that "richer people from the coast or the capital use derogatory terms to refer to us, saying we are low classes, making fun of our accent and skin tone." This has a profound impact on participants, as Grappa (17, male) stated that this kind of treatment "makes you feel like you're a nobody." Furthermore, participants noted how bullying had a greater impact on people with low self-esteem. While participants largely referred to Facebook as a main platform for negative messaging and bullying, other social media platforms, such as Instagram and Tiktok were also cited.

"The boys in my class have this game whereby the boy who leaves the classroom last gets slapped by all the boys. This is then posted online for everyone to see." (male, 13)


Bullying can also include body shaming, as an Emeritus Professor key informant "there was an overweight girl in the school in which I taught. Her schoolmates posted a video of her body shaming her. This impacted her negatively. The school administration only reacted by speaking to the culprits but they did not receive any real consequences for their actions" (interview with researcher). Furthermore, this empirical FG research also corroborates literature pointing to the intrinsic links between online and offline violence, as children FG participants highlighted instances when offline bullying and violence move online, and in turn, further perpetuate offline violence. For instance, Swayah (13, male) stated that "the boys in my class have this game whereby the boy who leaves the classroom last gets slapped by all the boys. This is then posted online for everyone to see." Participants agreed this has psychological and physical impacts as it is humiliating for the victim while perpetuating real-world violence against him.

31 Begley, J. (2014) "Connect: the development of an online social network for people on the autism spectrum and their families". Good Autism Practice. 15: 2.

32 Howard, P. L., & Sedgewick, F. (2021) 'Anything but the phone!': Communication mode preferences in the autism community. Autism. 25:8, 2265-2278

33 Pavlopoulou, G., Usher, C., & Pearson, A. (2022). 'I can actually do it without any help or someone watching over me all the time and giving me constant instruction': Autistic adolescent boys' perspectives on engagement in online video gaming. British Journal of Developmental Psychology, 40, 557-571. <https://doi.org/10.1111/bjdp.12424>

34 Dunckley, V.L. (2016). Autism and Screen Time: Special Brains, Special Risks: Children with autism are vulnerable to the negative effects of screen time. Psychology Today. <https://www.psychologytoday.com/us/blog/mental-wealth/201612/autism-and-screen-time-special-brains-special-risks>




As Anatole (13, male) stated “you will become known as fair game for everyone else to hit you and bully you.”

In addition to highlighting children’s experiences of bullying, the findings also draw attention to the importance of adequate and appropriate measures taken by schools, and more broadly, in response to bullying and cyberbullying, to protect the victim and to address the behaviour on the part of the bully.

3.3. Hacking

Participants frequently cited hacking as a risk. In particular, their passwords can be determined or extracted by “hacker links,” which deceive users to click on them only to steal their passwords. Once a hacker has access to an account, participants noted the potential harm that can be done to their personal data and to their reputation (if their accounts are commandeered). Importantly, participants also expressed their knowledge of how to protect themselves against these risks but admitted that there should be improved awareness of the risk and the need to train children on how to avoid hacking, such as avoiding using their real names when creating accounts and identifying the signs of a suspicious link.

3.4. Sexual Harassment



Sexual Harassment was a mostly gendered risk with male respondents reporting not being particularly affected. On the other hand, girls are the target of online sexual harassment, through body shaming, receiving unsolicited messages and pictures, or having their pictures which they had posted on social media reposted in Facebook groups with inappropriate captions and comments. As Touta (17) reported, she posted a picture of her face on her Facebook page, only to find it on another FB page with an inappropriate caption of a sexual nature. Participants noted that most security breaches and unsolicited contact they experienced occurred on Facebook. It is worth noting that, while sexual harassment discussions mostly occurred in girls only FGs, responses to the anonymous survey questionnaire administered to children at the end of each focus group reveal that the majority of all respondents have been subjected to unwanted sexual encounters on the internet.

Of the 108 children responding to the question “I saw or received a sexual message, picture, or video that I didn’t want to receive”, 66/108 said yes. This indicates 61% of respondents have been subjected to unsolicited sexual content (please see graph below).

I saw a message, photo or video on sexual character that I did not want to receive

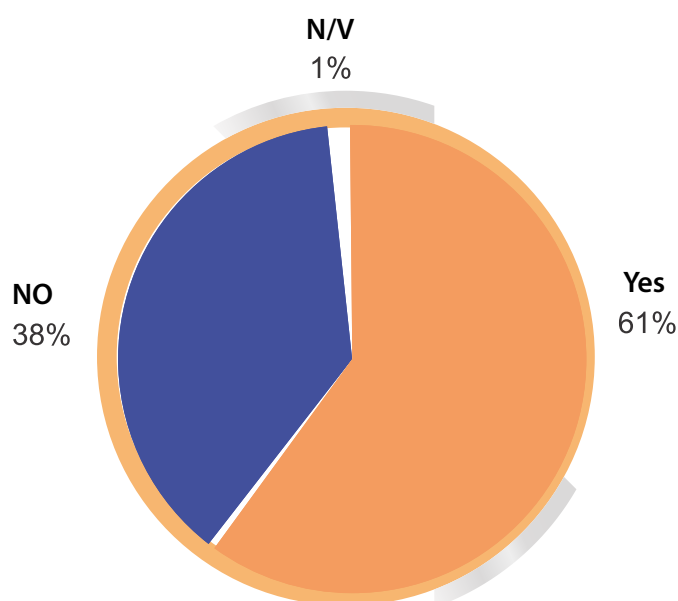


Figure 1: Survey responses to Q6

In addition, 36 respondents provided qualitative responses to survey question 19: "I have had bad experiences online that I would not want to talk to anyone about." These mostly relate to cases of bullying, hacking (fake profiles) unsolicited sexual images, sexual harassment, image-based abuse, defamation, and extortion (see Annex 5 for a full list of responses to survey question 19).

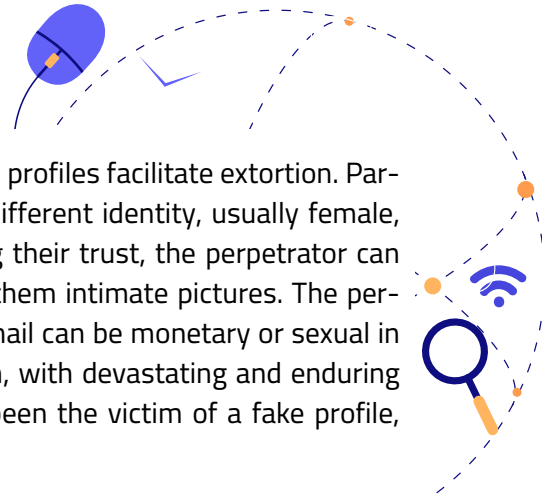


3.5. Fake Profiles and Extortion

Fake Facebook profiles were also discussed as a key threat facing girls on the internet. This can happen when someone uses someone else's pictures (which could be available on social media) to create a profile assuming their identity and sending inappropriate messages to their contacts and posting inappropriate content. Participants reported that they know many people who fell victim to this, including some of the participants themselves. This leads to problems and loss of friendships for the victim.

Marceline (14) reported that someone took her Facebook picture, photo-shopped her face onto explicit images, and then opened a new Facebook account pretending to be her. When explaining this distressing experience in the focus group, she burst into tears. Notably, Marceline explained that she resorted to telling her mother, as she was worried about further potential problems. However, her mother, who participated in a parents FG, did not mention this incident. This might indicate that the mother chose not to publicly talk about this issue, in front of researchers and peers.


However, it could also indicate parental denial of these matters, perhaps due to possible societal shame. This may also link to parental reticence to report instances of extortion with real or fake pictures for fear of potential reputational risks.




In addition to causing harm, FGs data showed how Fake Facebook profiles facilitate extortion. Participants described how this occurs when someone assumes a different identity, usually female, and befriends their female victims on social media. After gaining their trust, the perpetrator can convince the victim to have video chats with them and/or send them intimate pictures. The perpetrator then blackmails the victim with this material. The blackmail can be monetary or sexual in nature. Several participants reported having this happen to them, with devastating and enduring psychological impacts. A participant from FG5 reported having been the victim of a fake profile, which resulted in her blackmail for four years.

Rihan (14) shared a story she experienced two years prior to the FG. A (supposed) female befriended her on Tik Tok, then moved their conversations to Facebook where she started to convince her to send intimate pictures of herself. She assured Rihan that “it’s OK because we are both girls.” The perpetrator also entrapped Rihan by taking screenshots of a video call initiated by the perpetrator in which Rihan was fully clothed but the person on the other end of the line was naked. When Rihan was eventually convinced to send intimate pictures of herself, the perpetrator started blackmailing her and trying to contact Rihan’s family. The psychological impact is still clear on Rihan, who broke down in tears as she recounted her victimisation. Notably, her story spurred other participants to come forward, recounting their victimisation under very similar circumstances when they were 12 years old. Indeed, Marceline also broke down in tears stating “the same thing happened to me.” Kira also stated that a female acquaintance online tried to convince her to send pictures when she was 12. Kira, however, demonstrated her resilience by refusing and then blocking the person.


Notably, both victims reported that the perpetrators also tricked them into clicking on pornographic links or looking up sexual acts. This research found no systemic data on the extent of online extortion or its impact on victims. However, this phenomenon carries alarming trends, as child psychiatrist Dr. Fatma Charfi noted “we encounter a high number of girls with suicidal thoughts due to (sexual) extortion” (interview with researcher).



In addition to the psychological impact of falling victim to these schemes, all female participants exhibited a lack of knowledge about where or how to get help, and legal rights in such situations. When alerted to the fact that they can report these crimes, they all stated that they would not want to report for fear of being blamed by their families and the police. Indeed, Rihan, who said that she eventually spoke to her mother about what happened to her, said “until now, my mom is holding this against me and keeps blaming me. I don’t have a good relationship with my mother because of this.” In addition to fear of families’ reactions, there is a general perception of the police as not helpful in these situations. As Nawel stated “we all know what happens in police stations. If you go there to report someone for threatening to share intimate pictures of you they will probably blame you for taking those pictures in the first place” (17, female). This is an important finding for addressing non-reporting, and for creating a system and climate where children feel safe to report, and can do so without fear of reprisals and recrimination.



Male and female participants agreed that girls are disproportionately affected by fake profiles seeking to extract photos and videos for extortion purposes. Male and female participants also agreed that patriarchal societal norms mean that women and girls are held accountable when they fall victim to extortion due to the notions of honor associated with a girl’s body. As Grappa pondered “if someone shared my pictures, no one will care because I am a boy” (17). In addition, these same societal norms constitute a barrier to reporting.



However, boys are victimized differently by fake profiles. Some male participants revealed that they know many friends who had been lured by a fake profile pretending to be a girl seeking to meet in person. When the victim goes to the meeting in person, they are mugged by a guy or a group of guys.


6.6. Normalizing violence and online radicalization

For FG participants, the risks are also related to teenagers venturing into the dark sides of the internet, such as the dark web, pornography, and “Only Fans.” This can lead to ‘brainwashing’ of teenagers or personality and behavioral issues. Within this context, some FG participants cited being inadvertently exposed to highly disturbing and inappropriate content on social media, such as a TikTok account dedicated to posting videos depicting the murder and dismemberment of people. As Melissa stated, “I once saw a video of someone killing and disemboweling a small child. That really affected me negatively for a long time” (17, FG6).

In addition, children FG participants discussed the potential lasting impacts of exposure to violent material or ideologies on impressionable teenagers. While normalization of violence through games and videos was raised during children, parent, and teacher FGs, as well as key stakeholder interviews, these were largely discussed as a non-intentional form of violence (lacking intent to harm) which impacts children differently. However, other, more intentional, forms of manipulation were raised, such as radicalization into violent or non-violent religious extremism. Child judge Asmahan Boudhrioua, who specializes in counter-terrorism cases, confirmed that “while radicalization of adults largely happens offline such as in the mosque, most children are radicalized on social media. The initial phases of radicalization usually happen on Facebook then the children are asked to move to the more secure app Telegram” (interview with researcher).

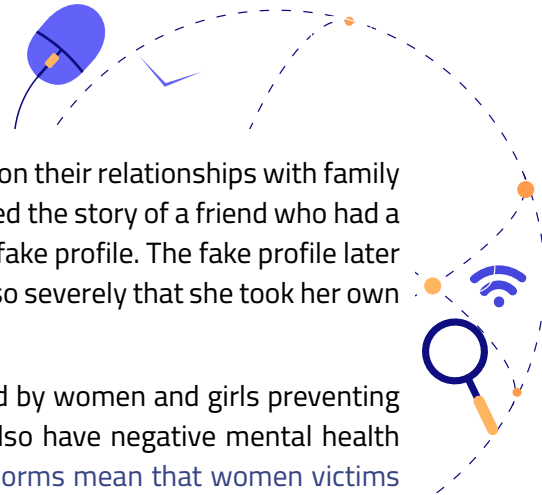


7.7. Mental Health risks



Participants discussed the various ways negative online experiences can impact their mental health. It was broadly noted that negative messages, trolling, and bullying have detrimental impacts on their self-esteem and mental health, **making mental health impacts is a risk which cuts across all other risks discussed above.** Participants criticized the “fake” lifestyles perpetuated by social media users pretending to be richer or happier than they really are. This can reduce their self-esteem as they compare themselves to unachievable standards. Also, some female participants reported that the “toxic positivity,” perpetuated by influencers on social media, harms viewers’ mental health, as it leads them to have unrealistic body image and lifestyle expectations. Despite exhibiting an awareness that the lifestyles and beauty standards they encounter on social media are “fake,” participants viewed that “if you’re exposed to these ‘stories’ every day they’re bound to affect you negatively” (Souhir, 17, female). The impact is reduced self-esteem as children compare themselves to unachievable standards.

“Mentally we are a lot older than our age because we are carrying problems we shouldn’t have to be dealing with at our young age.” (Mayar, 16)



Participants discussed the negative impact that fake profiles have on their relationships with family and friends. In an especially tragic example, one participant reported the story of a friend who had a relationship online with someone for years but turned out to be a fake profile. The fake profile later blackmailed her with pictures and videos. This affected the victim so severely that she took her own life.

In addition to the aforementioned extortion harm, obstacles faced by women and girls preventing them from reporting or discussing crimes they are a victim of, also have negative mental health impacts. Indeed, participants agree that **the patriarchal societal norms mean that women victims will be blamed and further victimized for being blackmailed with compromising pictures and videos.** This means that most victims do not feel safe enough to discuss these issues with their families or to report them to the authorities. Consequently, the victim continues to suffer the crimes in silence, with negative impacts on her mental health. As Mayar stated, “mentally, we are a lot older than our age because we are carrying problems we shouldn’t have to be dealing with at our young age” (16, FG5).

III. Prevention and response to online risks and harms facing children

While all children participants reported both positive and negative experiences while using the internet, focus group discussions revealed a high level of awareness and agency amongst children, who largely viewed themselves as wielding the power to reap the benefits of the internet while putting measures in place to prevent or respond to any risks and harms.



1. Children’s existing approaches to online protection

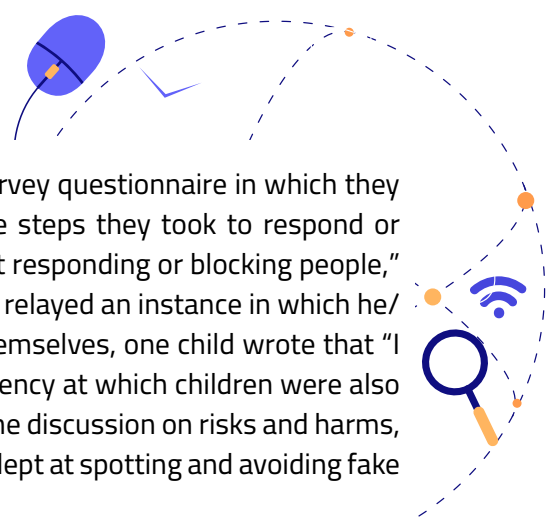
The majority of children FG participants demonstrated an awareness of the types of personal information available about them on the internet, including their names, age, gender, friends, things they like and don’t like, email accounts, locations they visit and where they live, their face and their pictures, their families, and where they go to school. As one participant in FG6 summarized, “the internet knows everything about us!” (Rose, 17).

“The internet knows everything about us” (Rose, 17).



1.1. Active measures children take to protect themselves online


Across children FG, participants discussed various measures they put in place to protect themselves include creating a secure Facebook account, withholding their real information on social media, including their real age and home address, not authorizing apps to access their data, not accepting people they don’t know on social media, keeping their photos private, and reporting any suspicious profiles or content. For instance, as participants in FG2 joked, they are experts at identifying the telltale signs of a fake Facebook profile, such as a heavily filtered and unrealistic profile picture, very few likes on pictures and posts, and a very recent account with a small number of “friends.” This vigilance is then followed by action to ward off risks, including blocking and reporting suspicious



accounts. Some of the children's responses to the anonymous survey questionnaire in which they recounted negative encounters on the internet also included the steps they took to respond or protect themselves, such as "you can solve these problems by not responding or blocking people," or "I told my mom and she was thankfully understanding." Having relayed an instance in which he/she were enticed by a fake profile to send intimate pictures of themselves, one child wrote that "I refused and deleted her from my friends list." However, the frequency at which children were also reporting scams and themselves being fooled by fake profiles, in the discussion on risks and harms, suggests that in practice, many children are not as practiced and adept at spotting and avoiding fake Facebook profiles as they might believe themselves to be.


"Sometimes I make it a point to use up all my 3G data on my phone so I can no longer be tempted to go online" (Arin, 17).

Similarly, participants, mainly female, voluntarily put concrete measures to self-moderate their internet use during the school year, including limiting gaming to the summer holidays. Others have resorted to unconventional measures to limit their internet use. As one female participant from FG8 stated "sometimes I make it a point to use up all my 3G data on my phone so that I can no longer be tempted to go online." (Arin, 17). Across FGs, children participants acknowledged that excessive internet use can be avoided through engagement in extra-curricular and outdoors activities and hobbies. This was corroborated by the fact that participants who did engage in such activities, such as sports or music, spent the least amount of time online.



However, these activities are not often available or possible for all children, especially for children from less privileged socio-economic backgrounds. In addition, the lengthy amount of time children across the target age group spend in school or in tutoring sessions were consistently cited by children and parents as depriving children of the time and energy for any extra-curricular activities. As FG participant Chahad illustrated, "I finish school at 6pm on many days, then I have two hours of tutoring outside of school, then I must go home and do my homework" (13, FG13). The result is children are so mentally and physically exhausted that "if I'm done with school related activities by 9pm all I have the energy for is to scroll through Facebook for a couple of hours in bed" (Maria, 17, FG8).

1.2. Help and knowledge seeking



Notably, the majority of children reported relying on the support of their friends and peers in cases in which they are subjected to online risks and harms, rather than discussing their problems with their parents. This is consistent with literature examined in the literature review (Annex 2) which reveals that children largely seek assistance or knowledge from peers rather than parents. This could be traced to the perceived and actual "digital gap" between parents and children, in addition to the lack of open and judgment-free dialogue at home. Indeed, "in all countries, the rapid pace of technological innovation undermines parental competence, this is, in turn, undermining children's willingness to turn to parents for support."³⁵

³⁵ Livingstone & Byrne (2018) p.19

1.3. Tailored and differentiated measures for protection

In addition, participants recognized that online risks do not impact individual children in the same way or to the same extent. Some FG participants pointed to some underlying factors which make some children more vulnerable to particular risks than others. Participants in FG8 highlighted that the negative impacts of bullying and other negative experiences on the internet are reduced in people with higher self-esteem, making it necessary to cultivate children's resilience through improving self-confidence. This was corroborated in an interview with child psychiatrist Dr. Ahlem Belhadj, who argued that "not everything that can harm a child online is a form of violence. For instance, the phenomenon of online influencers is very negative, but its impact varies between children based on their personalities, their lived experiences, their family environment. It is usually a vulnerable child who is more negatively impacted." (Dr. Belhadj, interview with researcher).

IT IS NOTABLE THAT CHILDREN PRIMARILY SAW IT AS THEIR OWN RESPONSIBILITY TO STAY SAFE ONLINE, RATHER THAN UNDERSTANDING THE LIMITS OF THEIR OWN AGENCY AND RESPONSIBILITY, AND RECOGNIZING WHERE THE RESPONSIBILITY SHIFTED TO OTHERS, AND IN PARTICULAR, THE APP DEVELOPERS, SOCIAL MEDIA PLATFORMS AND OTHERS WITHIN THE DIGITAL TECHNOLOGY SECTOR.

As children FG participants argued, if users suffer from low self-esteem or are vulnerable to negative experiences online, they can put in place other preventative measures, such as avoiding interactions on social media in order to avoid reading negative messages. Overall, children across FGs also highlighted the users' responsibility in avoiding and reporting inappropriate videos, such as content promoting violence or hate. Relatedly, participants recommended following positive people on social media.

Notably, the majority of participants agreed that parental controls are necessary for younger children under 13. For instance, in response to being exposed to unwanted content and ads of sexual nature online, a 13-year-old boy participating in FG 16 pondered that "I wish my mom would take away my phone, so that I don't have to see these things anymore" (Antonio). Indeed, across children FGs, participants highlighted the need for parents and the family to limit the use of internet for young children and to monitor the websites and content to which they are exposed.

Focus group discussions revealed a general level of awareness and agency amongst children participants to implement preventative and responsive measures to address online risks and harms on the one hand, and an attendant lag in knowledge and understanding amongst parents of the online benefits, risks, and measures for prevention and response on the other. Further, interview data with key stakeholders revealed several current or previous examples of positive governmental and non-governmental initiatives for prevention and response to online violence. These are explored below, with a view to drawing lessons learned and recommendations to inform the National Action Plan. However, it is also notable that children consistently saw it as their own responsibility to take measures to stay safe, rather than understanding where their roles and responsibilities, and those of agencies begin and end, and where does the responsibility of other critical actors lie, especially the app developers and social media companies. This reflects the findings from East Asian countries, where children assume primary responsibility for their own safety, rather than recognizing both their own agency (and the limits thereof), and while failing to recognize the full extent of the responsibility of the technology industry.³⁶

³⁶ UNICEF East Asia and Pacific Regional Office and the Centre for Justice and Crime Prevention, 2019

2. Existing efforts and measures for prevention and response

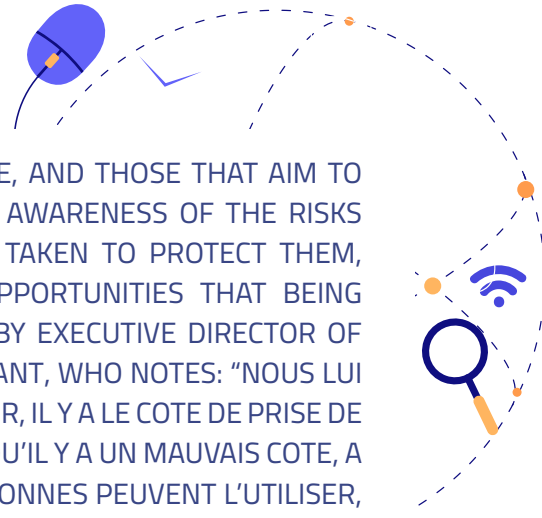
A number of initiatives and projects have been implemented by various Tunisian government institutions, civil society organizations, and with funding and support from international donors and INGOs to raise the awareness of children and parents around internet safety. For instance, in an interview with Mr. Lotfi Belazi, Executive Director du Centre National de l'Informatique pour l'enfant (CNIPE)³⁷, he outlined his center's past and planned awareness initiatives, he highlighted that raising children's awareness is a pivotal focus for there is no consistency across ALL document when it comes to the British and American spelling. There is a need to choose only one and to stick to it, and not alternate from the one to the other, cutting across all of their course offerings. As Mr. Belazi stated, «as far as raising awareness is concerned, these tools are present in all units.» (interview with research team).

The center ensures balancing children's awareness of the risks and harms associated with the internet with an appreciation of its benefits (see text box): "We are showing them the positive side. And when they manage to be positive, there's the side of awareness and sensitization [...]. And you have to know that there's a bad side, which is that if you share your data, other people can use it, that there are people out there who are on the lookout for these things, that there are also pedophile networks, and so on.» (Mr. Belazi, interview with research team).

Notably, interviews with key stakeholders revealed successful examples of inter-institutional coordination and collaboration to raise children's and parents' awareness about internet risks and safety. For instance, Mr. Anis Aounallah, Child Protection delegate, Tunis, recalled an awareness campaign which was implemented successfully between his office and the CNIPE. Similarly, Mr. Hichem Chebbi, general inspector within the Ministry of Education confirmed that his ministry has an established partnership with the CNIPE and its 24 regional centres across all Tunisian governorates.


As explained by Mr. Chebbi, primary and middle-school students are encouraged by their schools to visit the CNIPE or its regional affiliates to receive an array of ICT, programming, and robotics classes. "You will find some childre, from primary and secondary schools there. Some go on their own, others go via the schools." (interview with research team). However, it is worth noting that the regional centers are located in the governorate's centers and are therefore inaccessible to children from rural and remote backgrounds. In addition, as Mr. Belazi admitted, "The National Computing Centers or Regional Centers are not sufficiently present throughout the country, and do not have the services or a communication plan to make them more widely known to the public, whether among parents or children." (interview with research team).

³⁷ Le CNIPE est un établissement public à caractère administratif jouissant de l'autonomie administrative et financière sous la tutelle du MFFES




IT IS IMPORTANT THAT ANY AWARENESS RAISING INITIATIVE, AND THOSE THAT AIM TO FOSTER SOCIAL AND BEHAVIOURAL CHANGE, BALANCE AN AWARENESS OF THE RISKS THAT EXIST FOR CHILDREN ONLINE, AND THE MEASURES TAKEN TO PROTECT THEM, WITH AN EQUAL AWARENESS OF THE BENEFITS AND OPPORTUNITIES THAT BEING ONLINE PRESENTS FOR CHILDREN. THIS WAS EXPRESSED BY EXECUTIVE DIRECTOR OF THE DU CENTRE NATIONAL DE L'INFORMATIQUE POUR L'ENFANT, WHO NOTES: "NOUS LUI MONTRONS LE CÔTÉ POSITIF. ET QUAND IL ARRIVE A POSITIVER, IL Y A LE COTE DE PRISE DE CONSCIENCE ET DE SENSIBILISATION [...]. ET IL FAUT SAVOIR QU'IL Y A UN MAUVAIS COTE, A SAVOIR QUE SI TU PARTAGES TES DONNEES, D'AUTRES PERSONNES PEUVENT L'UTILISER, QU'IL EXISTE DES GENS QUI SONT A L'AFFUT DE CES CHOSES-LA, QU'IL EXISTE AUSSI DES RESEAUX DE PEDOPHILIE »

In addition to government-led initiatives, civil society and INGOs have also implemented awareness projects. For instance, Association "Sawn" for the protection of children and adolescents against violence and sexual abuse runs awareness workshops targeting children and their parents to raise their awareness and improve child-parent communication on issues related to sexual abuse. As Sawn president Mrs. Faouzia explained, these workshops aim to break down this taboo subject by « Let's explain to parents what the signs of sexual abuse are and how they can talk about it with their children. » (interview with researcher). In addition, interviews revealed a previous initiative undertaken by UNICEF in 2015 to raise the awareness of children, parents, educators and doctors about sexual violence against children. This initiative was discontinued following its adoption by the Ministry of Health, due to lack of resources and poor coordination between ministries.

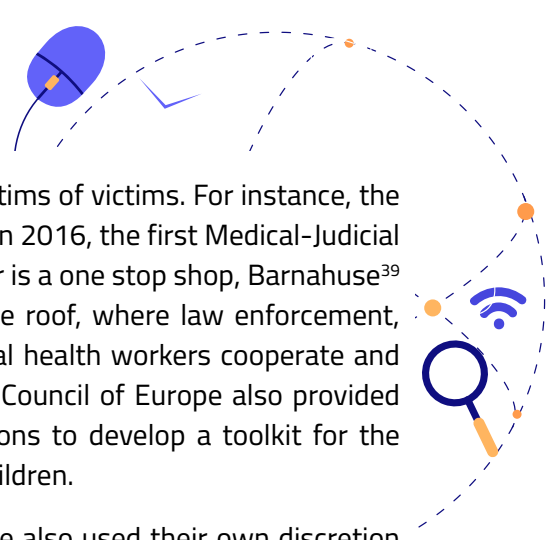


Interviews with key stakeholders revealed that, in addition to awareness raising, another important factor in prevention is to build children's resilience to online risks and harms through cultivating "soft skills" or "life skills." CNIPE general director Mr. Belazi views the advancement of children's soft skills as « A strategic issue that concerns the reform of society, and the restructuring of society as a whole! Because for us, as I've already said, soft skills are about helping children develop life skills. » (interview with research team).



This approach is being gradually integrated in the education system. As inspector general within the Ministry of Education Mr. Chebbi explained, the ministry is in the final inception phases of a cross-cutting and holistic program focusing on improving life skills in children in the first two years of primary education. According to Mr. Chebbi, « The aim of comprehensive health education is to protect children from all kinds of sexual abuse. One of the skills we're working on, and one that's very important, is decision-making.» (interview with research team). For instance, the new programme includes presenting children with fictitious situations to gauge their level of understanding of consent and teach them the types of situations which warrant them to refuse collaboration and speak to their parents. Notably, this program, titled "Santé Globale," is a repackaging of a previous initiative proposed by the ministry titled "Sexual Health" whose roll out was curtailed due to a societal backlash. Indeed, due to the initial branding of the program « It caused a senseless controversy. Parents thought we were going to teach children about sex. » (interview with research team). This suggests that awareness raising for parents, coupled with an improved communication strategy, is necessary for the successful roll out of these initiatives.

In addition to the abovementioned existing practices related to prevention, this research revealed

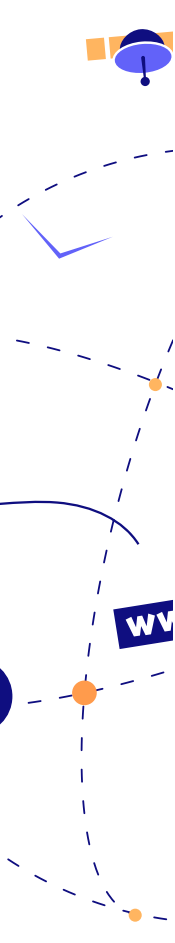


a number of positive initiatives for responding to and caring for victims of victims. For instance, the Council of Europe funded the establishment of the “Injed” center in 2016, the first Medical-Judicial Unit for women and children victims of sexual abuse³⁸. The center is a one stop shop, Barnahuse³⁹-style center which can provide a child-friendly office, under one roof, where law enforcement, criminal justice, child protective services, and medical and mental health workers cooperate and assess together the situation of the child and decide upon. The Council of Europe also provided funding to the National Body for Combating Trafficking in Persons to develop a toolkit for the detecting and caring for victims of human trafficking, including children.

In the absence of funding, actors involved in child protection have also used their own discretion to provide effective caring for victims. For instance, despite the absence of any de-radicalization programs or support for children, child judge Mrs. Asmahan Boudhrioua found a creative way to deal with cases involving children who have been radicalized online. As she explained, “we have an abandoned legal institution in the child protection code « مؤسسة الحرية المحروسة », j’ai utilisé le mécanisme de la liberté surveillée⁴⁰

I used the probation mechanism to set up a deradicalization program in collaboration with other volunteer partners.” (interview with researcher). This process included an assessment of the degree of radicalization of the child, psychological follow up, support to return to education or to join vocational training in coordination with the CPD and in close collaboration with the family. These efforts have proven successful. In her three years of applying this process, “We had zero cases of recidivism, and no child was ever involved in a terrorist case again. » (interview with researcher).

3. Legal and institutional gaps in online violence prevention and response



The mapping of the Tunisian legal framework (Appendix 3) revealed the existence of several legislative texts that deal with the issue of online violence against children, either directly or indirectly. These texts deal with the issue from different angles and are sector-based. At there is currently no legal text that deals with the issue in a holistic way, linking childhood and online violence. Thus, provisions relating to violence against children are scattered across several texts:

- Texts relating to violence against children (the penal code, the Child Protection Code, Organic Law no. 58 - 2017 of August 22, 6027 relating to the elimination of violence against women, Organic Law no. 61 of 2016 of August 3, 2016 on the prevention and fight against human trafficking, Organic Law no. 26 of 2015 of August 7, 2015 relating to the fight against terrorism and the prevention of money laundering) ;
- Texts relating to information/communication (Article no. 1 of 2001, dated January 15, 2001, promulgating the Telecommunications Code, Article no. 63 of 2004, dated July 27, 2004, on the protection of personal data, Decree-Law no. 115-2011, dated November 2, 2011, on freedom of the press, Decree-Law no. 2022- 54 of September 13, 2022, relating to the fight against offences relating to information and communication systems).

38 C’est dans cette unité que sont réalisés les examens médicaux exigés par les autorités judiciaires pour prouver la culpabilité de l’agresseur

39 A Scandinavian term for « children’s house”. Please see this link for more details.

40 La liberté surveillée stipule la désignation d’un officier chargé de surveiller l’enfant en conflit avec la loi.

3.1. Legal gaps

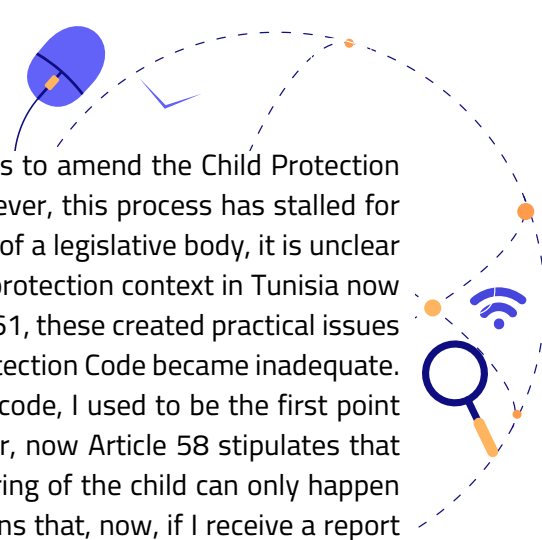
The lack of a specific legal text addressing online violence against children was not viewed as an inherent problem by most key stakeholders interviewed. As Mr Aounallah, CPD, Tunis stated “violence against children is codified in law, regardless of the means through which this violence is perpetrated.

In this sense, the response for online violence against children does not differ from the response to any form of violence against children” (interview with researcher). Similarly, Mrs Raoudha Bayouh, Ministry of Interior representative National Body for Combating Trafficking in Persons (INLTP) argued that «The problem is not legal. Whatever legal gap existed in online violence was filled by Decree-Law No. 2022-54 addressing cyber-criminality» (interview with research team).

In the same vein, family and child judges interviewed as part of this research assessed that they had the necessary legal basis to address cases of online violence, such as extortion, both for child victims and child perpetrators. As child judge Asmahen Boudhrioua, third-grade judge at the court of appeal, explained « articles 218 and 219 of the penal code criminalize physical violence, then Article 58 came to expand the definition of violence to include psychological violence” (interview with researcher). In addition, while Article 58 is essentially focused on gender-based violence, “the judiciary practice so far has applied this law for the benefit of children, even in cases where gender-based violence is not existent.” However, this “depends on the efforts and jurisprudence of each judge in applying the law” (interview with researcher). Similarly, family judge Sonia Jeridi stated that “the principle of the highest interest of the child is the magic bullet used by judges to leverage the existing legal tools for the benefit of the child” (interview with researcher). In addition, as child judge Boudhrioua pointed, international conventions to which Tunisia is signatory, such as the Lanzarote convention, are binding and can be used by judges in cases of sexual violence. For instance, before Article 58, judge Boudhrioua applied the Lanzarote convention to ensure that child victims of sexual violence are only interviewed once in the presence of a psychologist.

Notably, and due to the reliance on the jurisprudence, it is important to highlight the gap in the provision of specialized training for family and child judges on child protection. As child judge Boudhrioua highlighted, “judges do not choose their appointments but are often moved from different places to become a family or child judge. When I became a child judge, I did not receive any form of specialized training. I only know the Lanzarote convention because I did my homework and I received training from UNICEF between 2012 and 2014” (interview with researcher).


In addition, key stakeholders interviewed agree that the Child Protection Code is outdated and needs amendment to include the notion of victim. As Mr. Aounallah, CPD, Tunis, explained “there is a difference between a child victim and a child a situation of threat, and so the responses should be different” (interview with researcher). This is important because, as the literature review reveals, victims of online violence are at greater risk of becoming perpetrators of violence themselves. As child judge Jediri recalled “there was a case where a boy was extorting a girl from his school. The victim suffered mental repercussions as a result and so I ordered psychological follow up for her. However, it was also clear that the child perpetrator also had emotional issues... Our legal system views this boy as a perpetrator, but I also ordered psychological follow up for him” (interview with researcher). This highlights the need for effective identification and response to child victims, to prevent future violence. As child judge Boudhrioua argued, “generally, a child in a situation of conflict with the law is a child victim who received inadequate caring” (interview with researcher).




As confirmed by key stakeholders interviewed, there were efforts to amend the Child Protection Code to include a chapter on “child victims and witnesses.” However, this process has stalled for years and, due to ongoing political instability and the current lack of a legislative body, it is unclear when this process can be completed. In addition, while the child protection context in Tunisia now benefits from more advanced laws, such as Article 58 and Article 61, these created practical issues as the tools and mandate available to the CPD under the Child Protection Code became inadequate. For instance, as Mr. Aounallah, CPD, Tunis, explained “under the code, I used to be the first point of contact for children who are victims of sexual abuse. However, now Article 58 stipulates that the specialized police units are to be contacted and that the hearing of the child can only happen once in the presence of a psychologist or social worker. This means that, now, if I receive a report about a child being victim of sexual abuse, I am legally prohibited to listen to them” (interview with researcher).

Notwithstanding the legal gaps, the interview data also revealed a general agreement across key stakeholders about a gap in the implementation of the existing legal framework. This gap can be traced to an array of factors, each outlined in the sub-section below.

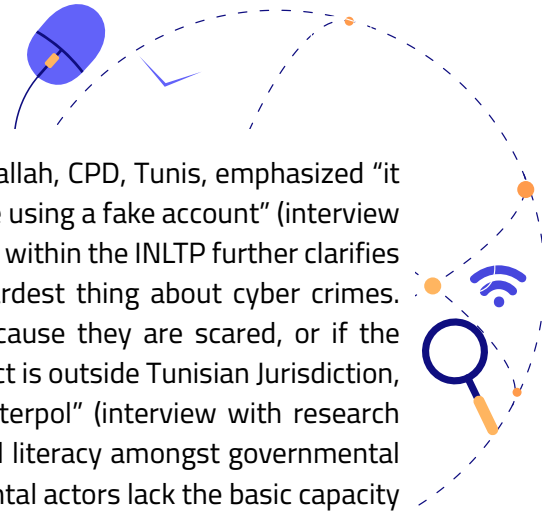
3.2. Gaps in knowledge and capacity amongst key child protection actors



Lack of knowledge and capacity for reporting among key actors: This research revealed a general lack of knowledge among relevant actors of the obligation to report suspected child abuse, and the anonymity of this reporting, as stipulated by Article 31 of the Child Protection Code. Findings from focus groups with teachers revealed their lack of knowledge about this obligation. Further, when teachers were aware of this obligation, they showed a reticence to report, for fear of harassment or retaliation by the perpetrator of the abuse or the child’s family. These fears can be perceived or real. As Mr. Mihyar Hamadi, General Delegate for Child Protection (GCPD), stated, there have been cases of teachers who were subjected to harassment after reporting abuse. Further, as Mr. Mihyar recalled “there was a case in which a teacher reported potential child abuse and the child’s family filed a complaint to the police against the teacher for defamation. The teacher was then summoned to the police station, and we had to explain to the police that the teacher was only fulfilling her legal duty to report suspected child abuse” (interview with research team). This suggests that **additional efforts are needed to increase the knowledge of educators and key child protection actors about mandatory reporting and response mechanisms.** As Mr. Aounallah, Tunis DPE, stated, “despite the Ministry of Education disseminating multiple memos to its staff about mandatory reporting, these memos do not reach the teachers, especially in remote locations” (interview with researcher). As Mr. Hamadi, GCPD, stated, there exists a Memorandum of Understanding (MoU) between the Ministry of Education and the MFFES. As part of this partnership, the “CPD offered to train educators and admin staff in schools about the obligation and process of reporting potential cases of abuses” (interview with research team). However, as of the time of writing, the CPD has not received a response.




Reinforcing the knowledge and capacity of educators on reporting and response mechanisms must be coupled with enhancing public awareness, including of children and parents, of online risks and safety, in addition to the existing legal safeguards and mechanisms in cases of child victimization. Such awareness initiatives can simultaneously contribute to prevention efforts as well as to identifying and responding to existing violence.



A technical and digital gap among response actors: As Mr. Aounallah, CPD, Tunis, emphasized “it is especially difficult to trace online criminals, especially if they are using a fake account” (interview with researcher). Mrs. Bayouhd, Ministry of Interior representative within the INLTP further clarifies that, “gathering the necessary evidence for conviction is the hardest thing about cyber crimes. This is often complicated if the victim deletes the evidence because they are scared, or if the suspect deletes the evidence or uses a fake profile, or if the suspect is outside Tunisian Jurisdiction, especially given the coordination problems we have with the Interpol” (interview with research team). These efforts can be further hindered by the lack of digital literacy amongst governmental actors. For instance, Mr. Aounallah stated that “a lot of governmental actors lack the basic capacity to use digital technologies. I previously didn’t know that if someone sends me video evidence of child abuse on Facebook that I should download it on my phone right away. I learned this the hard way when a video I was sent was deleted at source and I lost the evidence. I had to teach myself how to deal with these technologies” (interview with author). This reflects the general lack of integration of digital tools across the administration. For instance, as Mr. Aounallah explained, “a lot of government institutions still deal with fax. I’ve sometimes had to send pictures through fax, and when they arrive, they are dark and impossible to discern” (interview with researcher).


Therefore, the technical nature of online violence necessitates an overhaul of human and material digital capacity to ensure effective response. As Mrs. Bayouhd, Ministry of Interior representative within the INLTP highlighted, “the new cyber-criminality law came to fill the legal gap in dealing with online crime. In theory, we have institutions such as the Tunisian Agency for Internet and specialized units within the Mol to deal with cybercrimes. In practice, these actors lack the technical means to effectively address these highly technical crimes” (interview with research team).

3.3. Lack of psychological support for children



Children participants in focus groups consistently highlighted their need to **access to psychological support**. However, interview data revealed a **gap in the provision of psychological support to children and victims of violence**. According to the majority of key stakeholders interviewed, the numbers of psychologists within the Ministries of Health, Aducation, and Social Affairs are deficient. Further, as child psychiatrist Dr. Fatma Charfi stated, “the number of psychologists affiliated with the Ministry of Health could be sufficient if they were allocated efficiently. For instance, the ministry allocated psychologists to emergency rooms. However, these psychologists could be better utilized elsewhere where there is a more pressing need for them” (interview with researcher).

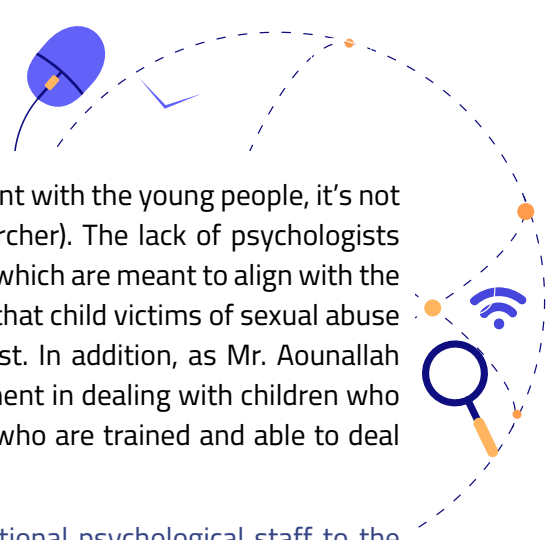
By contrast, structures which were designed to provide psychological support to children in schools, such as the BEC and the CEC.⁴¹ established by the Ministry of Health, have effectively never functioned due to the unavailability of psychologists. As a result, as president of the civil society organisation “Sawn” Ms. Faouzia Chaabane highlighted, “We went to work in Hay Hlel, Mallesin and Sidi Hsin, and each time, we found young people and parents in schools, completely lost and looking for psychologists.” (interview with author).



Further, as Mr. Aounallah, CPD, Tunis, explained, government affiliated psychologists are largely restricted to their offices and do not make field visits to schools or to children’s residence.

This was corroborated by Ms. Chaabane, who highlighted that «The psychologists working at the Ministry of Education and in the delegations rarely visit the schools. They should be in contact with

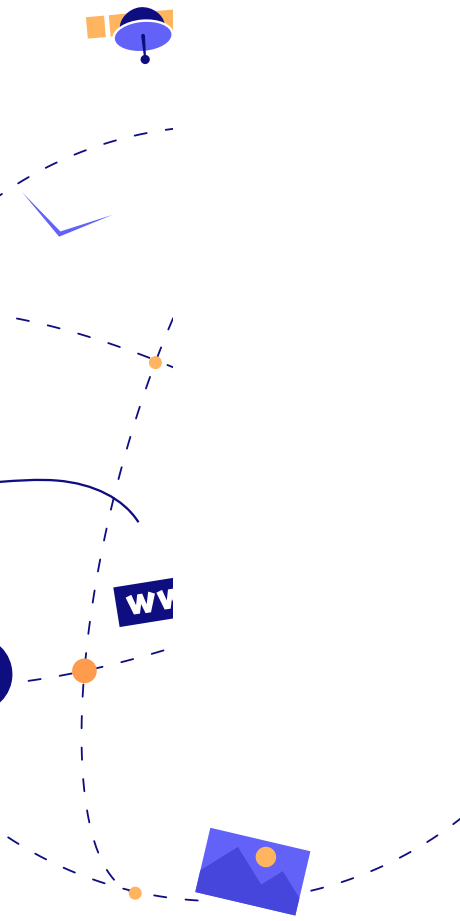
41 Ce sont des permanences médicales au sein des établissements secondaires ou supérieurs assurées par les médecins scolaires.



the children, not the delegations. The psychologist has to be present with the young people, it's not an administrative job.» (Faouzia Chaabane, interview with researcher). The lack of psychologists often defeats the purpose of initiatives such as the "Injed" center, which are meant to align with the stipulation in the Lanzarote convention and Article 58 mandating that child victims of sexual abuse are only to be interviewed once in the presence of a psychologist. In addition, as Mr. Aounallah highlighted "the lack of psychological support is especially prominent in dealing with children who have been radicalized. We always struggle to find psychologists who are trained and able to deal with these children" (interview with researcher).

While financial restrictions may prevent the recruitment of additional psychological staff to the ministries of health, social affairs, education, and MFFES, this research revealed that coordination with civil society can help bridge this gap. For instance, as Mr. Aounallah, Tunis DPE, explained, "we have worked with some CSOs, such as "les psychologues du monde" and "Health and Psychology," especially when we need to identify psychologists who are willing and able to go to the victim" (interview with researcher). However, as Mr. Aounallah stated, working with civil society actors can be challenging when their fundraising efforts lead to a breach of confidentiality. For instance, "I partnered with a civil society organization on a case of abuse once, and then I found that they published all of our communication and the specificities of the case online as part of their efforts to attract funding" (interview with researcher).

The recommendations advanced in the following section of this report are based on the existing practices and initiatives, and global best practice, in addition to the gaps identified in this section. This research process has revealed that an effective strategy for addressing online violence against children must focus on prevention as well as response.



IV. Recommendations

The burgeoning body of literature and evidence, as well as global guidance, on what works in preventing and responding to online violence against children, provides a useful framing for how the findings of this research can inform practical, realistic and achievable recommendations.

The recommendations below draw in particular on the INPIRE Strategies to End Violence Against Children, as well as the Model National Response (discussed in detail in the attached literature review), to ensure the alignment of the response with global and regional commitments and strategies – a particularly important consideration for protection in the digital environment, which by definition transcends national borders, and requires global and regional cooperation and collaboration. The recommendations provided below also provide a starting point for the development of the National Action Plan in a way that avoids siloes and duplication of efforts. As such, for each recommendation, this report identifies potential areas of synergies with existing governmental or non-governmental strategies and efforts.

Ensuring children’s voices are central to the development of all policy and legislation impacting on children in the digital environment. Given the intersection between the safety and wellbeing of children online, and all other aspects of their lives in the digital space, such as learning, play and civic participation, the centrality of children’s voices and experiences must be ensured across all these sectors if an effective and rights-based environment is to be created that ensures and enhances child online protection. The recommendations are divided into those relating to policy and legislation, systems strengthening, and prevention and response mechanisms.

1. Recommendations on research and data

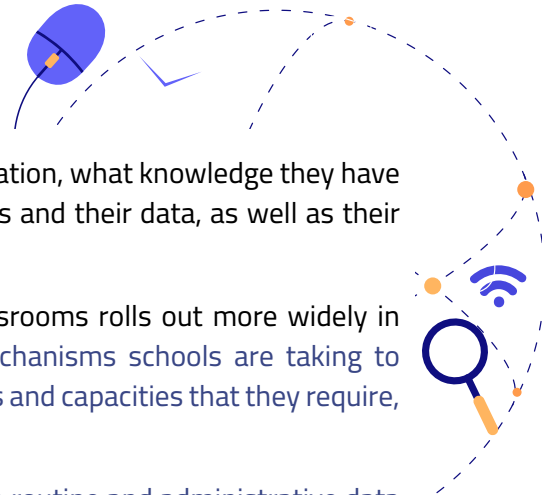


Often considered as secondary priority for policy making and legislating, quality research and good quality data is critical for good policy making, legislating and the design of appropriate, well-designed interventions. For this reason, these recommendations are highlighted first.

A reliable, representative baseline of the experiences, both positive and negative, of the online experiences, opportunities, skills and harms of all children in Tunisia, should be established. This study has highlighted the importance of widespread consultation, and the importance of having reliable and representative data on children’s experiences using the internet and digital technology. While this study was qualitative in nature, and is not representative of all children in Tunisia, it provides a glimpse into some of the existing concerns, gaps and priorities in keeping children safe, as well as some of the institutional and structural challenges. This will allow for baseline data to inform the monitoring of the National Action Plan on Child Online Protection, as well as to inform the design of appropriate interventions. The upcoming Disrupting Harm (DH) study provides a tangible opportunity to do this.



While Disrupting Harm provides the opportunity to collect and utilize the representative data required to better monitor and implement legislation, policy and programming, it will be important to ensure that more detailed, qualitative data, such as that collected in this study, is gathered at regular intervals to provide the nuance and depth of quantitative data collected through DH. In particular, a greater understanding of children’s understanding of data privacy and protection is



required in order to better assess how children are sharing information, what knowledge they have of privacy, and what steps they take to better protect themselves and their data, as well as their personal information, online.


Similarly, as EdTech and other uses of digital technology in classrooms rolls out more widely in Tunisia, more research will be required on what steps and mechanisms schools are taking to safeguard children online, to equip children with the changing skills and capacities that they require, and to protect their data.

Data collection, and regular monitoring, must be incorporated into routine and administrative data collection processes, such as school-based data and the move to an integrated case management system within the child protection system, that allows for any issues related to children's use of technology are recorded and reported on.

2. Policy and legislative recommendations


Some level of legislative reform is required in order to achieve the level of legislative compliance and consistency envisaged (and required) to address sexual and other forms of online violence within a child-rights framework envisaged in the MNR and other global frameworks. Tunisia is in an enviable position within the region by virtue simply of its stated commitment and history of prioritising children's rights within its legislative and policy framework, and this can be leveraged to further develop regional best-practice.

2.1. Ensuring consistency across instruments and laws

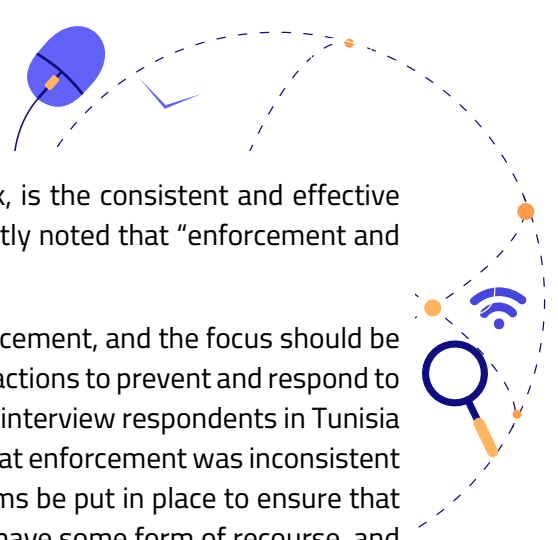


Legislation should be reviewed and where necessary, amended, to ensure consistency across instruments and laws, as well as consistency with the most recent legislative guidance and knowledge. Consistency is required across legislation in order to ensure common standards by different actors within the protection, law enforcement and judicial response to online violence, and where possible to avoid judicial and prosecutorial discretion. While this may bring advantages, it also may result in the application of unequal standards and remedies depending on the individuals involved. The application of common standards, definitions and consistent law minimizes the potential for this. Several respondents in the study noted the suitability of the existing law, within the context of judicious application, yet also noted the need for some reform, and the existing application of discretion by judges.

This research revealed that the role and tools available to the CPD, as enshrined in the Code of Child Protection, are no longer compatible with the requirements of more recent legislative texts such as Article 58 and Article 61. Therefore, it is necessary to review response and prise en charge mechanisms in view of the new legislative landscape, in order to overcome procedural confusion and overlap and to reassert the CPD's role as a point of first contact with children.



In addition, a consistent and equitable enforcement of existing laws and policies must be applied, and accountability mechanisms formulated for when this is not the case.



As important as ensuring a comprehensive legislative framework, is the consistent and effective enforcement of laws relating to online violence. It has been recently noted that “enforcement and regulatory action may be more influential than legislation itself.”⁴²

It is common cause that legislation is only as effective as its enforcement, and the focus should be as much on equipping all responsible actors to take the mandated actions to prevent and respond to all forms of violence affecting children in the digital space. Several interview respondents in Tunisia noted that the existing legislative framework was adequate, but that enforcement was inconsistent and at times lacking. It is important that accountability mechanisms be put in place to ensure that where the law is not appropriately or adequately applied, victims have some form of recourse, and that government and government agencies are held accountable for the enforcement of laws and regulations.

2.2. Prioritizing the reform of the Child Protection Code

It is necessary to introduce the notion of child victim to the existing legal framework related to child protection. While it is difficult to overcome the political instability which has played a role in slowing down this process, it is important to relaunch this process and including civil society in consultations related to the addition of a third chapter to the code related to child victims and witnesses. Several specific considerations should be integrated, amongst others:


- Associated with the above, ensuring the protection of child victims who may be criminalized as victim when self-generated content is shared non-consensually, as image-based sexual abuse (discussed further below).
- Ensure recourse for victims of online child sexual exploitation and abuse.



Best practice on child online protection in Australia, Ghana, and Cambodia

In Australia, the Online Safety Act requires any online service provider, from social media companies and internet service providers, to take reasonable steps to keep children safe online, including responding within 24 hours to requests for take-down orders of CSAM, to responding to reports of cyberbullying or other risks. Failure to do so can result in civil penalties or other penalties. Provisions for penalties and fines on telecommunication services providers who do not take adequate steps to keep children safe online have also been incorporated into recent legislation in Ghana, through the cybersecurity act of 2020. Another alternative currently being explored in Cambodia, is the incorporation of similar obligations in licensing agreements for ISPS and other ICT and digital service providers within their licensing agreements. Failure to meet these obligations would result in operating licenses being withdrawn, or penalties imposed.

42 WHO, 2022, pg. 10



This process falls under the mandate of the MFES as the lead agency, but in order to ensure a coordinated protection system response, it is important to involve, at a minimum, civil society, the Ministry of Education, Ministry of Justice, Ministry of Interior, Ministry of Health, Ministry of Telecommunications and the Cyber-crime Unit, as well as the upcoming legislative body and Prime Minister's office (to ensure the prioritization of this reform).

2.3. Establishing Industry Guidelines for online child protection

A common, equitable approach to child online protection for the digital technology and ICT industry, with accompanying Industry Guidelines must be established, to ensure compliance to their obligations to keep children safe online, and to take appropriate action and measures to prevent and respond to online violence. These Guidelines should apply to both Tunisian and global companies, and should be consistent with global best practice. They should take into account measures such as safety and privacy by design, age-appropriate content, age verification and other emerging and recent developments relating to Industry to meet their obligations to keep children safe (Where is the text box?). Such obligations must be developed in consultation and with agreement of the digital technology companies and related bodies within Tunisia.

3. Capacity building and systems strengthening



The need for the capacity building and training on child online protection, child rights as they translate in the digital space, and in some instances, on digital skills, consistently emerged from this research. All training recommended below could be accredited with sector-relevant bodies for continual learning and professional development points, thus raising the incentive for participants. Three distinct target groups were identified for training:

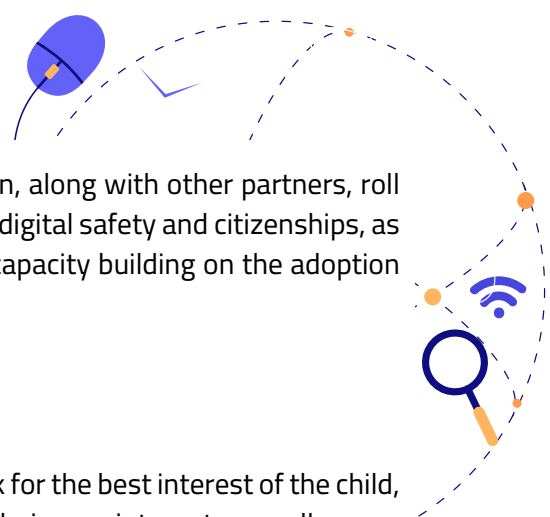


3.1. Training for Educators

Several areas requiring capacity building were identified, including an understanding of the range of children's rights that can be realized online, the need for a more nuanced and complete understanding of the risks children face (including those that may be presented by the growing use of digital technology in the classroom (through EdTech), and privacy issues), the potential harms, effective rights and evidence-based strategies, and in some instances more complete digital skills.

Existing initiatives include Where is the text box? , but training is also required to identify signs of distress and trauma within the classroom, and on the reporting of violence and online exploitation and abuse when they do become aware of it. Further, with a view to bridging the gap in available psycho-social support and capacity and resources for children, particularly outside of Tunis, select educators may receive specialized training and qualification to act as a counselor or a first point of contact with children seeking psychological and emotional support.






This training is increasingly important as the Ministry of Education, along with other partners, roll out pilot and other trials of the use of tablets in classrooms. Basic digital safety and citizenships, as well as privacy and data protection skills, must form part of any capacity building on the adoption and use of these new technologies in the classroom.⁴³

3.2. Training for child and family judges


Due to the pivotal role they play in interpreting the legal framework for the best interest of the child, child and family judges must receive specialized training prior to their appointment, as well as periodically, including on international conventions ratified by the Tunisian government.

3.3. Digital literacy and COP training for public officials

This will require a cultural and material shift across all Tunisian governmental institutions to digitize records and communications. However, existing digitization efforts are sectoral in nature, such as Security Sector Reform donors (such as the USIP and the UNDP) providing equipment and training to the Ministry of Interior to enhance digitization. For the purposes of this National Action Plan, and in view of advancing realistic targets, this recommendation focuses on improving the digital literacy of CPDs and other key actors involved in child protection.

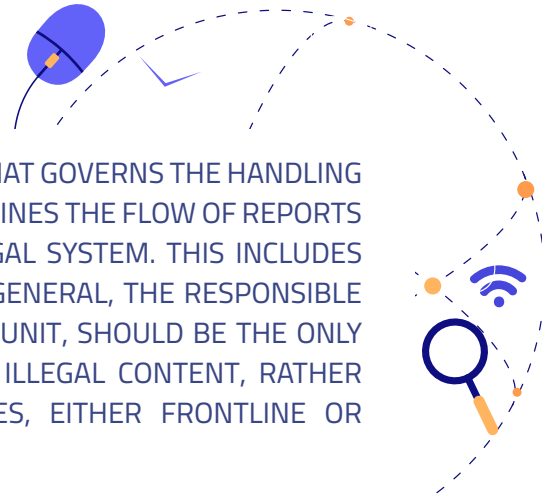


However, one gap emerged in particular from the study that warrants a particular mention. This relates to the skills required, and the procedures involved, when reports are made, or when CSAM or other digital content involving children, is identified. A very explicit protocol (with training) is required that governs the handling of content in a way that minimizes views and streamlines the flow of reports and content through the child protection and legal system. This includes how and when content should be downloaded. In general, the responsible law enforcement agency, the cybercrime unit in Tunisia, should be the only mandated agency responsible to engage with any illegal content, rather than others within the child protection services, either frontline or administrative. This is also important for evidence retention and handling.



This is both a training gap and a procedural and protocol gap, as there is no clear guidance that officials are aware of to determine the management of CSAM or other harmful content. This gap likely undermines the potential for any successful prosecution of cases, where illegal content or behaviour is involved, and undermines the potential for due protections to be provided to the victims (including protections relating to privacy and confidentiality, and the re-victimization and traumatization that may occur when sexual content, in particular of a child, is viewed unnecessarily by those in a duty of care). It is important that all those in a duty of care, from frontline protection officers to educators, are aware of the reporting processes and restrictions on their own handling and viewing of materials and should thus be a consistent component of all training, not just for child protection workers or public administration officials.

⁴³ Useful guidance on the use of EdTech can be found in new UNICEF guidance here: United Nations Children's Fund, 'Child Protection in Digital Education: Policy Brief', UNICEF, New York, January 2023. <http://www.unicef.org/documents/child-protection-digital-education>



A VERY EXPLICIT PROTOCOL (WITH TRAINING) IS REQUIRED THAT GOVERNS THE HANDLING OF CONTENT IN A WAY THAT MINIMIZES VIEWS AND STREAMLINES THE FLOW OF REPORTS AND CONTENT THROUGH THE CHILD PROTECTION AND LEGAL SYSTEM. THIS INCLUDES HOW AND WHEN CONTENT SHOULD BE DOWNLOADED. IN GENERAL, THE RESPONSIBLE LAW ENFORCEMENT AGENCY, IN TUNISIA THE CYBERCRIME UNIT, SHOULD BE THE ONLY MANDATED AGENCY RESPONSIBLE TO ENGAGE WITH ANY ILLEGAL CONTENT, RATHER THAN OTHERS WITHIN THE CHILD PROTECTION SERVICES, EITHER FRONTLINE OR ADMINISTRATIVE.

3.4. Training on responsible child-rights focused reporting for journalists

Through the validation process for this report, the importance of responsible, child rights-focused reporting on children's online experiences, risks and harms was highlighted. This corresponds with the findings of this study in the sense that much of the narrative and perceptions of children's experiences online was facilitated by media reports and suggests the need for targeted training for journalists on how to responsibly report on children in the news. The manner in which children's experience online risks and harms, including reporting on specific incidents, can both undermine victims right to privacy and protection from further harm, and serve as a vehicle for misinformation. In South Africa, Media Monitoring Africa has developed both accredited and non-accredited training for mid-career journalists on responsible child-centred reporting, which could serve as a model for similar training in Tunisia.⁴⁴ This is further supported by a children's reference group which regularly monitors and comments on reports involving children in the media.

4. Prevention and response mechanisms



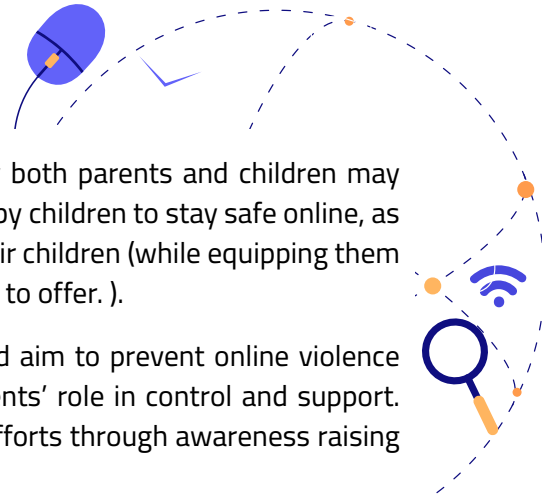
The recommendations relating to response and prevention services address three inter-related areas: strengthening the child protection system with a particular focus on psycho-social services for children, social and behavioural change, incorporating awareness and prevention education, and support for parents and caregivers, and children themselves.

4.1. Launching awareness campaigns targeting children and parents

Both parents and children in Tunisia exhibit a level of awareness of many of the risks that children may face online. Adult's attitudes and awareness tend to focus more on the risks and harms that digital technology presents to children, and many children tend to be more aware of these aspects of digital technology.

A greater investment in awareness and Social and Behavioural Change (SBC) programming that includes online safety and child online protection is required. These include universal awareness programming, but also, more targeted social and behavioural change strategies targeting some of the known drivers and risk factors for online violence. The findings of this research reflect many of the fear-based misconceptions and incorrect messaging that are often disseminated in a well-meaning attempt to keep children safe.

⁴⁴ Media Monitoring Africa (2022) Empowering Children in the Media. Children Youth and Media. <https://mediamonitoringafrica.org/empowering-children-in-media/>




The awareness of common (and unsubstantiated messaging) by both parents and children may undermine the actions, knowledge and decision-making required by children to stay safe online, as well as the actions taken by parents and caregivers to support their children (while equipping them with the skills required to make the most of what the Internet has to offer.).

Awareness raising should target children and parents and should aim to prevent online violence through awareness related to internet risks and safety and parents' role in control and support. In addition, awareness campaigns must contribute to response efforts through awareness raising about legal protection and support mechanisms for victims.

Ultimately, these awareness campaigns should seek to break down taboos and obstacles to reporting extortion and sexual harassment, while reinforcing a culture of open and safe dialogue between parents and children.

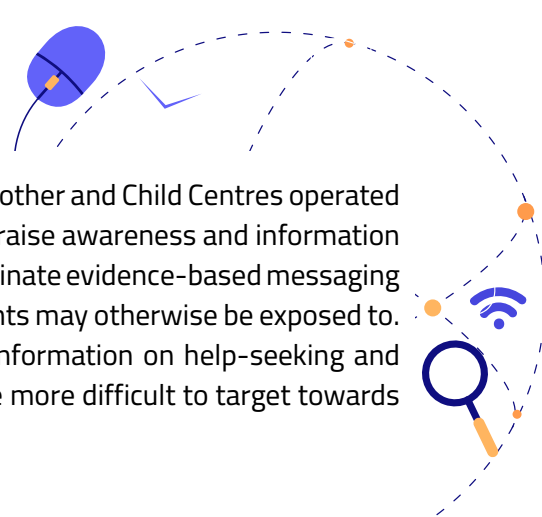
Parents and teachers must be made aware of the wealth of opportunities and benefits that the internet offers to children, and the importance of the internet and digital technology to realizing the wide range of rights that children have. The research revealed far greater awareness of the risks and potential harms that face children online, with very limited awareness of the wealth of advantages, a result possibly of primarily fear-based messaging and information that parents are exposed to. Messaging should also try to avoid fear-based messaging, which has been shown to yield no positive outcomes and be ineffective.

In tandem, targeted support for parents and caregivers, including from conception through to adulthood, should be provided. Evidence increasingly points to the importance of supporting parents and caregivers of very young children, in how best to support their children as they first start to engage with digital technology. This ranges from how children of different ages can best engage with digital technology, the sort of activities that are appropriate at different ages, the amount of time spent online doing different activities, and how digital technology, when used appropriately at different ages, can aid and foster development and skills.



Integrating basic digital literacy, digital parenting and safety skills into ECD and parenting programming can yield substantial benefits for both children and parents.⁴⁵ Existing initiatives in partnership with the Government of Tunisia offer opportunities to integrate digital safety into existing programming with minimum additional investment and offering a favourable cost-benefit outcome. One example is the existing ECD partnership between UNICEF and the Government of Tunisia to pilot ECD programming in four sites. An additional benefit of integrating online safety to messaging into such initiatives is the opportunity to reach social or child protection frontline workers as well as parents or caregivers. Examples of these that could be applied to the prevention of online violence include those that yield positive outcomes for dating violence, sexual violence and bullying, specifically.

⁴⁵ It is important to differentiate between digital literacy, media literacy and online safety. The focus of each is different, and each set of skills require different competencies, although they may overlap. Care must be taken not to collapse online safety into digital literacy interventions, for example. This is discussed in more detail in Finkelhor D, Walsh K, Jones L, Mitchell K, Collier A. Youth Internet Safety Education: Aligning Programs With the Evidence Base. Trauma Violence Abuse. 2021 Dec;22(5):1233-1247.




In Tunisia, planned initiatives to incorporate ECD messaging into Mother and Child Centres operated by the Ministry of Health also offer easy wins to disseminate and raise awareness and information on how best parents can support their children, as well as to disseminate evidence-based messaging rather than ad-hoc messaging unsupported by evidence that parents may otherwise be exposed to. Such an approach also provides an opportunity to disseminate information on help-seeking and reporting of CSAM or other forms of abuse that may otherwise be more difficult to target towards caregivers.

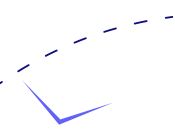
4.2. Improving children's resilience to online risks and harms

This research found evidence of existing, albeit nascent, governmental programmes and initiatives focusing on improving children's resilience, which can be built upon, such as the Santé Globale programme initiative and the CNIPE offerings. Notably, as this research report finds, it is important for the CNIPE and its regional centers to improve their reach and exposure through the design and launching of a communication strategy.

Ultimately, similar centers should be launched outside governorate capitals to facilitate access to children from rural and remote areas. Awareness raising can also build on the existing initiatives of the Ministry of Education, Ministry of Telecommunications and Agence Nationale de la Sécurité Informatique, and the Telecommunications companies and ISPs.

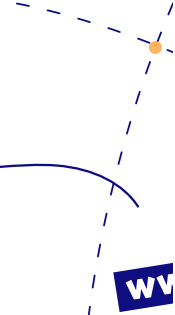


BUILDING ON THE RECOMMENDATIONS OF THE RECENT WORLD HEALTH ORGANIZATION STUDY OF BUILDING ON THE EFFICACY AND IMPACT OF INTERVENTIONS TARGETING SEXUAL VIOLENCE IS THE EXAMPLE OF CURRICULUM-BASED INTERVENTIONS IN LOW TO MIDDLE-INCOME COUNTRIES THAT TARGET SEXUAL PSYCHO-SOCIAL RISKS AND ADDRESS MULTIPLE RISK AND PROTECTIVE FACTORS AFFECTING SEXUAL BEHAVIOURS (SUCH AS KNOWLEDGE, PERCEIVED RISKS, VALUES, ATTITUDES, PERCEIVED NORMS AND SELF-EFFICACY). THESE HAVE BEEN SHOWN TO CONSISTENTLY HAVE POSITIVE OUTCOMES ON CHILDREN, AND CAN BE ADAPTED TO INCLUDE MODULES, COMPONENTS AND EXAMPLES OF ONLINE VIOLENCE.



There is also evidence from elsewhere in the world that prevention education and awareness raising can yield positive outcomes in preventing online violence, from both the victim and offender perspective. Similarly, given the intersection between the drivers for violence against children, and online violence against children⁴⁶ there is a high likelihood that SBC interventions for the prevention of violence against children will yield similar positive outcomes for online violence.⁴⁷ Tailoring evidence-based interventions and programming that have been shown to work to integrate online protection components will likely yield similarly positive outcomes on online safety.

In Tunisia, this may entail the incorporation of wider school-based curriculum and extra-curricula programming that focuses on respectful relationships, empathy, good decision-making, conflict resolution and communication, ultimately fostering greater child resilience.⁴⁸



⁴⁶ Maternowska et al; WHO, 2022.

⁴⁷ WHO, 2022, pg.15

⁴⁸ Within the MENA region, these subjects are addressed through life skills and citizenship education (LSCE). Conceptually, LSCE sets out to equip children and young people with a set of skills across different dimensions, at an individual, social and instrumental level. The subject builds on the notion of four cluster of skills essential for growth and development: skills for learning, skills for personal empowerment, skills for active citizenship, and skills for employability. Within each of these sets of skills are "Core life skills". All of these have direct bearing on online safety. Skills for learning generally includes creativity, critical thinking, and problem solving; skills for employability includes negotiation, conflict-resolution and cooperation, and skills for active citizenship include respect for diversity, empathy and participation, and skills for personal development include self-management, resilience and communication. Each of these

4.3. Enhancing psycho-social support provision for children

Given the lack of state financial resources, this can be achieved by 1) reinforcing the role of specialized civil society actors, through increased collaboration with the CPDs, to fill the gap in psychological support provision. This must be undertaken through partnership agreements which compel civil society actors to maintain the confidentiality and anonymity of children, 2) improved allocation of existing government affiliated psychologists and child psychiatrists, and 3) reactivating the BEC and the CEC..

Given the capacity constraints and limited number of government frontline social workers and child protection workers, leveraging the reach and capacity, and willingness, of civil society organizations in providing quality services to children may be important. While no organizations focusing specifically on online risks, or the online experiences of children, were identified in the course of this study, several organizations providing broader prevention and response services to children expressed willingness to support government in providing psycho-social and protection services. Such organizations could provide valuable assets in ensuring that more services reach more children.

5. Institutional recommendations

The Model National Response is explicit for the need for inter-sectoral collaboration and appropriate mechanisms to ensure this happens, in any effective OCSEA strategy. The same applies to all aspect of child online protection. The following recommendations relate to institutional considerations.

5.1. Ensuring inter-government coordination on child online protection

Child protection online should be integrated into all ministries involved in any activities with, or providing services to children, including MoE. In the case of Education, this is particularly so as the Ministry pilots the use of tablets and ICT within schools. In Jordan, the Ministry of Education introduced an online protection training programme for all teachers within the context of COVID, as education shifted online.⁴⁹

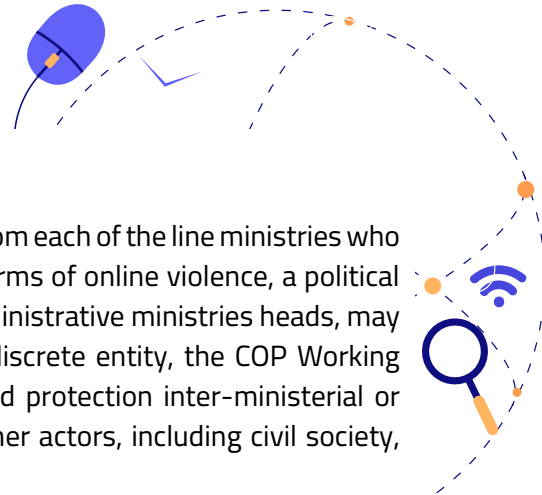
While this process is in its early stages in Tunisia, introducing online protection measures, and building the capacity of teachers from the outset, will become increasingly important. Global guidelines on the Child Online Protection and the use of EdTech provided by UNICEF can be a valuable starting point for this process.⁵⁰

The existing steering committee, established for the purposes of this project, provides an excellent starting point for a coordinating mechanism to oversee the implementation of these recommendations, as well as to support and drive the NAP. However, it is important that a Child Online Protection Working Group or coordinating body, has the political weight and authority to drive the NAP.

sets of skills is evident in most evidence-based youth and child violence prevention programmes, even if not yet in programmes targeting VAC. See UNICEF Middle East and North Africa. 2017. Analytical mapping of life skills and citizen education in the Middle East and North Africa. Life Skills and Citizenship Education Initiative. UNICEF MENA: Jordan. Available at <https://www.unicef.org/mena/reports/analytical-mapping-life-skills-and-citizenship-education-mena>

49 <https://www.unicef.org/jordan/reports/online-safeguarding>

50 United Nations Children's Fund, 'Child Protection in Digital Education: Policy Brief', UNICEF, New York, December 2022.




As the NAP is likely to require commitment (including budgetary) from each of the line ministries who are involved in a comprehensive response to OCSEA and other forms of online violence, a political head who can engage on an equal footing with ministries and administrative ministries heads, may be required. It is also proposed that rather than standing as a discrete entity, the COP Working group or coordinating body be a sub-structure of a broader child protection inter-ministerial or departmental working group. Finally, it will be important that other actors, including civil society, industry and research bodies are represented on this structure.

5.2. Integrating online protection into the formal child protection mechanism

The strengthening of the child protection system and establishment of an integrated case management system is already underway in Tunisia and online risks should be integrated into this process. This can form the basis of strengthening the protection system to ensure readiness and capacity to adequately deal with those cases of sexual and other forms of online violence that require formal child protection intervention or management.

Given the complexity of behaviour and risks attached to activities such as sexting and self-generated images, it is important that both the child protection and judicial system are responsive to the needs of children, and the special circumstances and protections that they require. One way of managing this is to ensure child-friendly courts and “one-stop” centres, which protect the anonymity, confidentiality of children, minimize re-traumatization, and encourage reporting within a safe environment where children can be guaranteed as far as possible no stigmatization. The Child Judges in Tunisia have already received considerable training on child-friendly justice. This provides an important entry point to enhance the judicial response to online extortion and other forms of potential criminal and procedural issues relating to children in the digital environment and COP, particularly within the context of one-stop centres.

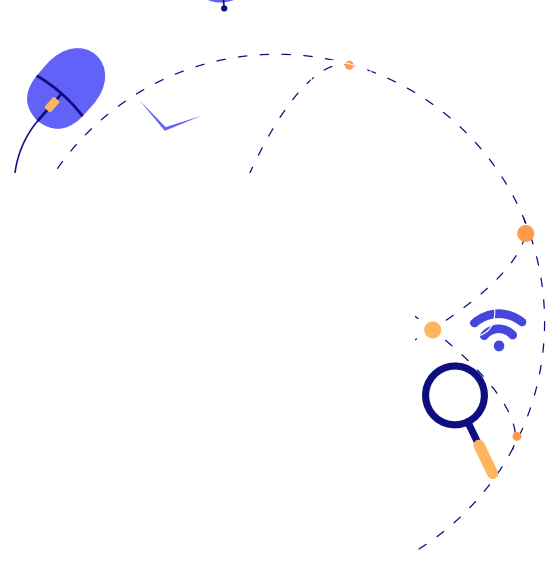


In Tunisia, the Council of Europe partnership with the Ministry of Justice to implement the Barnahus one-stop centres can provide an initial entry point for training and supporting the protection and judicial response service on online protection.

While the model has not been evaluated specifically for positive outcomes on children reporting online sexual abuse or who are involved in cases entailing online extortion, the model has been identified as a promising practice for enhancing service provision and justice for children who are either (or both) victim or perpetrator.⁵¹

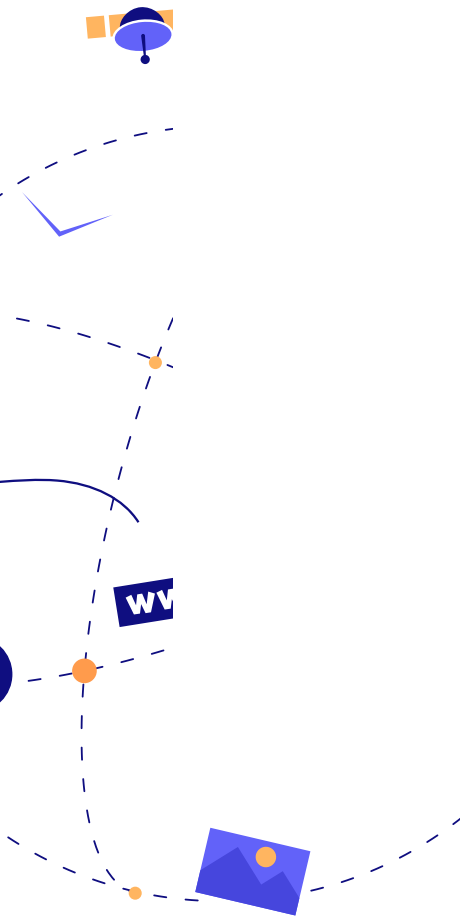
Focusing on targeted support for justice officials, from judges, prosecutors, police and child protection officers, within these select sites will also facilitate the collection of reliable data on cases, and how these are managed within the integrated child protection system, and ultimately, provide a useful departure for an evaluation of such interventions specifically on online safety outcomes.

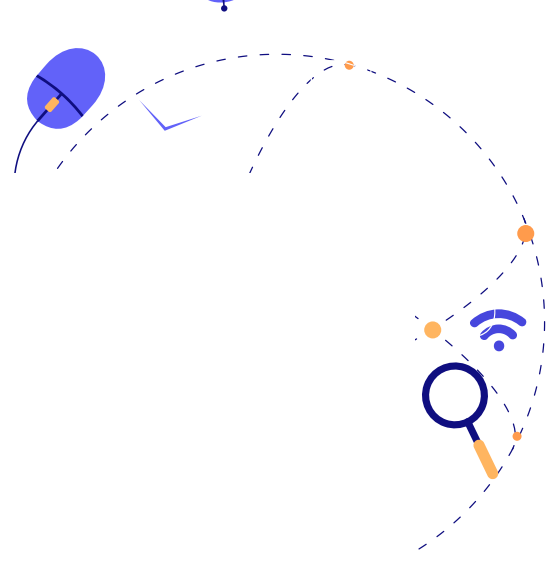
⁵¹ United Nations Children’s Fund (2021) Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York. p. 32.



List of Annexes

- **Annexe 1:** Conceptual Literature Review
- **Annexe 2:** Legal Literature Review
- **Annexe 3:** Detailed discussion of research site selection





Appendix 1 : Literature Review



I. Introduction

This literature review was prepared as part of a research study that will be used to develop a national action plan for the prevention of online violence against children in Tunisia. This research is conducted by the Centre for Justice and Crime Prevention and Resolve Consulting for UNICEF Tunisia and the Ministry of Women, Family, Children and Seniors - MFFES).

1. Analytical approach

This literature review is based on peer-reviewed scientific literature, administrative data generated by the Tunisian government or international/regional organizations and institutions, and reports from industry experts. Relevant legislation and policies in various sectors, including security, justice, social welfare, education, religious affairs and information technology, are also reviewed. This review places particular emphasis on identifying existing government policies and measures for the incorporation of all aspects related to the identification, prevention and response to online violence, and the degree of their alignment with global guidelines and frameworks (including the MNR and INSPIRE, as well as terminology advice and a framework for children's rights as set out in GL.25), taking into account the Tunisian and regional context. This aims to identify gaps, as well as the potential need for harmonization between legislation and policy.

2. Limitations

This is a literature review that selectively identifies key texts and broad coverage of studies on online child protection, the implementation of a «child rights approach», the links between online and offline violence, how online risks can lead to both online and offline harm, and the maintenance of children's rights in balancing the risks and opportunities associated with depriving children of access to technology.

However, as this research is not as comprehensive as a systematic review of the literature, it is plausible that not all best practices or international studies were included. In addition, the literature reviewed contains a bias towards English studies, but the reports, laws and strategies in French and Arabic of Tunisian ministries and research agencies are also analyzed in Annex 2. Sonia Livingstone's work is widely featured in this journal because she is a leader in the field who has made outstanding theoretical and empirical contributions.

II. Children online in Tunisia

Tunisia's population is 11.9 million, of which 20.3% (about 2,433,970) are between the ages of 5 and 17. Tunisia has an internet penetration rate of 66.7%. Of the 8.15 million social media users, 7.1 million use Facebook, the third most visited website, after Google and YouTube.¹ Notwithstanding regional disparities, the use of the Internet, and in particular social networks, is predominant among Tunisian children and adolescents. According to a 2017 survey,² Tunisian teenagers aged 15 to 17 use the internet 3 to 5 days a week on average, while 43.9% use social media daily.

Despite the documented rise in online violence against children globally, a UNICEF report highlighted the lack of specific systemic data on online violence affecting children in Tunisia.³ This highlights the lack of a clear strategy and mechanism to identify and document the various forms of online violence and threats targeting children. This, in turn, hinders any attempt to effectively combat this phenomenon while taking into account children's right to access and benefit from the Internet.

The COVID-19 pandemic has highlighted the importance of digital technology in children's lives. The lockdown periods have forced children to spend more time online and have significantly reduced their opportunities to play outdoors, meet friends and family outside of their immediate family, or engage in social physical activities. Interaction with friends and peers at school has been similarly reduced, with schooling shifting, to a large extent, to the online space.

The pandemic has also highlighted existing inequalities in access to technology and broadband, especially outside urban centres. This impacts both access to technology and technology infrastructure, but also the digital literacy of children and youth online.

In Tunisia, historical regional socio-economic inequalities have been compounded by a «digital divide» that disadvantages marginalized children in poor interior regions. Children represent 29% of the Tunisian population, they represent 40% of the country's poor. In addition, children living in rural interior areas are at increased risk of living in (extreme) poverty. This precariousness has been further exacerbated by Covid-19, with poverty rates raising from 15.2% to 19.1% and extreme poverty from 2.9% to 3.3%.⁴

These conditions lead to a multidimensional precariousness of children and to the entrenchment of regional disparities. For example, due to inequalities in access to health care, rural interior regions have higher infant mortality rates (19/1000 compared to 11/1000 in urban areas in 2018).⁵ Unequal access to adequate infrastructure and education services has resulted in interior regions suffering from higher drop-out rates at primary and secondary level and higher failure rates at the baccalaureate. Dropout rates for children in poor interior regions are 2.5 times higher than average. In 2021, the wealthiest coastal regions of Sousse and Monastir recorded baccalaureate pass rates of 61% and 62.5% respectively, while rates in the inland regions of Tataouine (southeast) and Jendouba (northwest) were 38.6% and 35.7% respectively.⁶

1 Kemp, Simon (2021) Issue 2021: Tunisia. DataReportal. <https://datareportal.com/reports/digital-2021-tunisia#:~:text=There%20were%207.92%20million%20internet,at%2066.7%25%20in%20January%202021.>

2 UNICEF Tunisia (2020) Analysis of the situation of children in Tunisia. p. 128 <https://www.unicef.org/tunisia/rapports/analyse-de-la-situation-des-enfants-en-tunisie-2020>

3 Ditto.

4 Ministry of Women, Family and Senior Citizens (2021) Integrated Public Policy for the Prevention and Protection of Children Project. p. 4 <http://www.femmes.gov.tn/wp-content/uploads/2017/07/Resum%C3%A9-excutif.pdf>

5 Ditto, p. 4

6 BAC Tunisia (2021) Success rate by section and region. <https://www.bac.org.tn/bac-tunisie-2021-taux-de-reussite-par-section-et-par-region/#:~:text=On%20retrouve%20par%20la%20suite,2%20avec%2055%2C31%25.>

Unequal access to the internet and IT tools has reinforced regional socio-economic inequalities that existed during the pandemic. For example, «children (...) equipped with appropriate equipment (computer, printer, and Internet access allowing virtual teaching) will be better disposed to fill the teaching deficits caused by the closure of schools and high schools for several months.»⁷

These inequalities in turn generate and exacerbate other inequalities that can directly put children at greater risk of various types of violence. Children with lower levels of digital literacy may be disadvantaged if education were online, resulting in lower academic performance than their peers, which represents a violence risk factor. These children may also be more vulnerable to certain types of violence that occur both online and offline, such as online child sexual exploitation.

III. Online Risks and Harms: Key Considerations

Despite some definitional issues, there is a general consensus in the literature and policy that online risks can be operationalized into three categories: content, contact and conduct. In addition, based on recent developments and a growing body of evidence on the commercial and privacy risks faced by children online, a fourth category can be added, namely contractual risks.⁸

- **Content risks** include those where children interact with or are exposed to potentially harmful content;
- **Contact hazards** describe all cases where the child experiences or is exposed to potentially dangerous adult contact;
- **Behavioural risks** refer to scenarios in which the child himself participates or is the victim of potentially harmful behaviour by his or her peers;
- **Contractual risks refer to risks** to which children are exposed when they are involved in potentially harmful contractual risks or may be exploited by them.

The table below shows the CO:RE classification of the main online risks affecting children, according to the four categories mentioned above.⁹

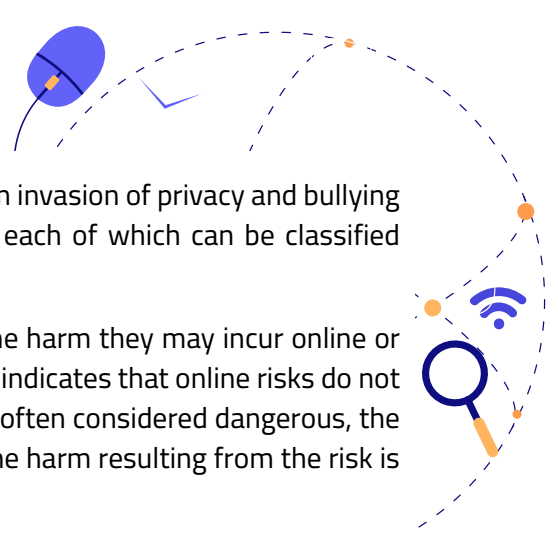
7 Mahjoub, Azzam (2020) Covid 19 pandemic in Tunisia: Inequality, vulnerabilities to poverty, and unemployment. Tunisian Forum for Economic and Social Rights. p.9 <http://ftdes.net/rapports/COVID-AZ19.pdf>

8 Livingstone Mascheroni and Staksrud, (2015); Staksrud and Livingstone, (2009)

9 Livingstone Mascheroni and Staksrud, (2015); Staksrud and Livingstone, (2009)

Sonia Livingstone and Mariya Stoilova, «The 4Cs: Classifying Online Risk to Children», CO:RE Short Report Series on Key Topics (Hamburg, Germany : Leibniz-Institute Für Medienforschung | Hans-Bredow-Institute (HBI), 2021), 12, <https://doi.org/10.21241/ssoar.71817>.


KERNEL	Content	Content	Content	Content
	Children interact with or are exposed to potentially harmful content	Where the child experiences or is exposed to potentially dangerous adult contact	The child himself participates or is the victim of potentially harmful behaviour by his or her peers	Children when they are involved in potentially harmful contractual risks or may be exploited by them.
Aggressive	Violent, bloody, graphic, racist, hateful, or extremist information and communication	Harassment, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity. Example: online insults, exclusion, humiliation	Identity theft, fraud, phishing, scams, hacking, blackmail, security risk.
Sexual	Pornography, (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual solicitation, sextortion, generation and sharing of child sexual abuse materials	Sexual harassment, non-consensual sexual messaging, adverse sexual pressure	Trafficking for sexual exploitation, streaming (paid for) child sexual abuse
Securities	Misinformation, age-inappropriate marketing or user-generated content	Ideological belief or manipulation, radicalization and extremist recruitment	Potentially harmful user communities, e.g. self-harm, anti-vaccine, adverse peer pressure	Gambling, filtering bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Transverse	<p>Violation of privacy (interpersonal, institutional, commercial)</p> <p>Physical and mental health risks (e.g. sedentary lifestyle, screen abuse, isolation, anxiety)</p> <p>Inequalities and discrimination (exclusion, exploitation of vulnerability, algorithmic bias, predictive analytics)</p>			




Online risks can include several different experiences, ranging from invasion of privacy and bullying to encountering racist, hateful, violent or pornographic content, each of which can be classified according to the typology presented below.¹⁰

The interconnection between the risks children face online and the harm they may incur online or offline is established in the literature. However, the literature also indicates that online risks do not inherently lead to harm online or offline. Although these risks are often considered dangerous, the risk is only an indication of the potential danger of the Internet. The harm resulting from the risk is a more accurate indicator of what makes the Internet unsafe.¹¹

One risk that often differentiates online abuse from offline abuse is when a child meets a stranger in person/offline that they first met online. The risks associated with this range encompasses sexual assault, abduction, as well as child sexual abuse equipment. In addition, there is a risk that the sexual solicitation took place before the meeting. Yet, meeting someone offline, in real life, when the contact was originally made online, is often one of the attractions of online chat or engagement. The Internet offers the opportunity for children, whether in traditional or integrated communities or in marginalized or isolated settings, to engage beyond their immediate circle or frame of reference. Data from the Global Kids Online study, a research conducted in four countries in the Global South, shows that 30% of children have met in person with someone they initially met online. Although these children were «at risk» when meeting a stranger, the study did not capture how many of them experienced some type of harm. Little evidence is available on the nature and extent of children's experiences of online harm. Indeed, very few studies have attempted to capture the prevalence of harm. After all, it's hard to operationalize and ethically capture data about the degree to which children are upset by what they encounter online. Others have used mental health checklists to capture the psychological harm that can result from online experiences. There are some exceptions to the general terms in which injury is generally analysed.



These tended to focus very specifically on the harms that might be associated with sexual harassment, exposure to pornography and cyberbullying.¹²¹³¹⁴¹⁵¹⁶



The extent to which risk translates into harm, and indeed the extent of the harm itself, is further complicated by the fact that risks and harms flow through the online and offline world. Livingstone argues that «for the most serious risks (such as sexual solicitation, or prolonged exposure to extreme pornography, or such sustained bullying that a child is driven to self-harm), it is often assumed that, although the risk is encountered online, the harm will occur offline.» This allows child protection agencies and intervention services to respond to the resulting harm as they would any other case of abuse. However, as the gap between online and offline life, in addition to online and offline risk and harm factors, blurs, response workers are increasingly required to consider how services encompass both online and offline spaces.¹⁷

10 Staksrud and Livingstone, (2009)

11 Staksrud and Livingstone, 2009; Slavcheva- Petkova (date) Nash & Bulger, 2015).

12 CJCP, 2012; Boyd, 2014

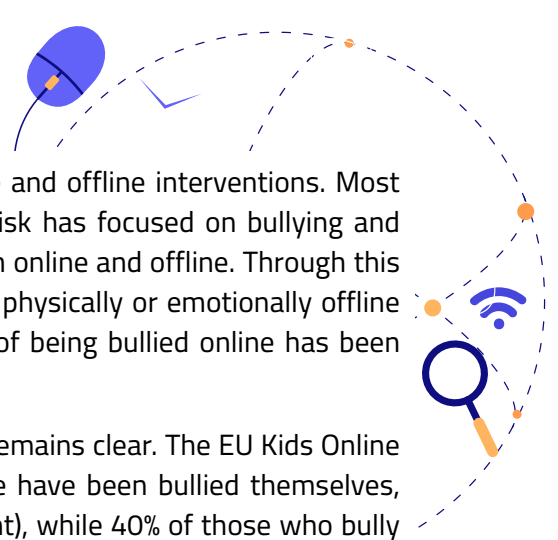
13 Global Kids Online (2017) Reference COMPLETE Required.

14 Livingstone & Helsper, (2010); Slavcheva- Petkova, Nash & Bulger (2015)

15 David Smahel et al. (2020) Survey results from 19 countries». EU Kids online. Doi: 10.21953/LSE.47FDEQJ010FO.

16 Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Review of the Empirical Research Literature. *Trauma, violence and abuse*, 19(2), 195–208.


17 Livingstone (2013)



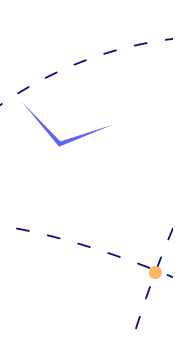
Bullying provides a useful context for examining effective online and offline interventions. Most work on exploring the relationship between online and offline risk has focused on bullying and cyberbullying, and the relationship between bully and victim, both online and offline. Through this body of work, the relationship between the risk of being bullied, physically or emotionally offline – often referred to as schoolyard bullying – and the likelihood of being bullied online has been established.¹⁸

The cyclical relationship between online and offline harassment remains clear. The EU Kids Online study showed that 60% of children who bully themselves online have been bullied themselves, online or offline (the space in which this happens is not significant), while 40% of those who bully online have been bullied online themselves. It is important to note that this also reflects the same risk that those who have been bullied online will become online bullies themselves, as has long been recognized in the offline space. Similarly, in the Optimus Foundation’s study on child abuse and neglect in South Africa, a strong relationship occurred between online and offline bullying. Those who were bullied were likely to have experienced this online and offline, as well as the experience of transitioning between online and offline.^{19,20,21,22}

Studies have also looked at the extent to which online risk emulates or spreads from offline risk and the extent to which offline risk predicts online risk. While comorbidity is increasingly documented, causal pathways are less understood. Children who report more risks offline are more likely to report more risks online, as well as be more likely to report harms resulting from encountering those risks online. violence, including sexual violence, exposure to violence and child abuse.^{23,24}



While it has been found impossible to determine causality or pathways (i.e. pathways from one form of online or offline violence to another, or which violence predates the other), existing research identifies the strong association between online violence and other forms of offline violence that may stem from several factors. The relationship between vulnerability and experience of multiple forms of violence (polyvictimization) and violence in different spheres (home, school, community) is well documented. Children who experience multiple victimization are more likely to experience trauma than those who experience a single incident or form of violence.^{25, 26}



Children exposed to violence or victims offline (including sexual victimisation) can use the online space to seek support and companionship, or establish safer relationships than offline relationships, in the same way that children who are socially isolated offline can form stronger relationships or find safe spaces online. However, despite the positive conclusion that children who suffer offline can find support and comfort online, other studies show that experiences of offline violence can also lead to depression, anxiety, and social withdrawal, and other trauma-related psychological outcomes have been shown to increase the risk for both cyberbullying and online sexual abuse such as sexual solicitation.²⁷

18 Wolak 2007

19 Patchin and Hinduja, 2006; Blacksmith et al., 2006; and Jang et al., 2013

20 Menesini, (2017).

21 Study Optimus (2016) Sexual abuse of children and adolescents in South Africa South: forms, scope and circumstances. UBS Foundation Optimus <https://www.ubs.com/global/de/ubs-society/philanthropy/blog/2018/child-sexual-abuse.html>

22 Burton et al., (2017).

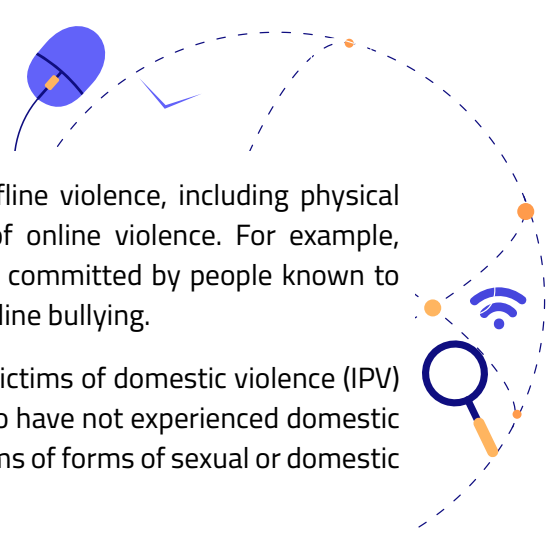
23 EU Studies and Global Kids Online -

24 Burton et al., next

25 Finkelhor et al. (2015), Leoschut & Kafaar, (2017)

26 Samms-Vaughan and Lambert (2017)

27 Merrill et al., (2016); Carve et al., (2013).



There are also common characteristics of different forms of offline violence, including physical and sexual violence, that are common to the characteristics of online violence. For example, interpersonal violence, sexual abuse and bullying are most often committed by people known to the child, a characteristic shared by children who are victims of online bullying.

A study on online bullying in the United States shows that adult victims of domestic violence (IPV) are more likely to be victims of online harassment than those who have not experienced domestic violence. It is therefore plausible that the experiences of child victims of forms of sexual or domestic violence are not different.²⁸

Despite studies showing how online actions can lead to offline consequences and vice versa, other publications establish how violence permeates the online and offline dimensions and is fundamentally interconnected. This intersection between online and offline violence is evident in the way violence is experienced, the nature of the violence and its impact on victims. Kardefelt-Winther and Maternowska present three scenarios to illustrate this point.

- **#1:** A child is sexually abused at home and the act is photographed. The images are sold online and widely shared. Is it a case of online sexual violence or sexual violence at home?
- **#2:** A child receives a hurtful threatening message on a social networking site. The child arrives at school feeling intimidated by his classmates. Is this cyberbullying, peer-to-peer violence, or school-related violence? »
- **#3:** A child sends explicit images to a partner, who shares them with classmates. The images have spread on social media and the child is being bullied. Eventually, the child commits suicide. Does this constitute online violence, sexual abuse or violence in schools? »²⁹



This section demonstrates that online violence comes in different forms and that the relationship between online and offline violence is often mutually constitutive. While exposure to risk can lead to harm, online risks are not intrinsically linked to online or offline harm. Therefore, as discussed in the next section, it is essential to ensure that children are aware of the risks and that their rights to access the Internet are not restricted.

IV. Ending violence against children while protecting their rights

Access to the Internet is a child's right. The deprivation of access to the Internet, in the 21st century, risks slowing down their development. However, the blurred distinction between online and offline means that it is «more complex than ever to determine how best to keep children safe» and that it is «difficult to advance evidence-based prevention and response.» To address this complex challenge, this section reviews the literature on children's vulnerability to online violence in addition to the right and the developmental need for children to have access to the Internet.³⁰

28 Ybarra et al, (2017)

29 Kardefelt-Winther, D., Maternowska, C. Addressing violence against children online and offline. *Nature Human behavior*. 4, 227–230 (2020). <https://doi.org/10.1038/s41562-019-0791-3>

30 Kardefelt-Winther & Maternowska (2020)

1. Children's vulnerability to online violence

Addressing online risks requires understanding whether certain factors or conditions increase the risk and thus make children more vulnerable to online violence. However, this is an exceptionally difficult task when the literature identifies the child's age, gender, sexual orientation, cognitive ability, behavior, location, and region of the world. In addition, the literature suggests that links between online and offline responses should be maintained.

First, «there is insufficient evidence to provide a clear indication as to whether the risks associated with online activities are the same or have the same implications for children in different parts of the world.» In addition to the different risks in different contexts, the risk is not static, and children do not experience it alone throughout their childhood. A review of educational materials for the prevention of child sexual exploitation and abuse in online and offline contexts provides insight into how risk experiences change over time. It demonstrates that the types and frequency of risks to which children are exposed, in addition to how children are likely to react, change throughout their childhood. «Children's internet use, behaviour and vulnerabilities differ according to their age.» Thus, children's vulnerability to risk evolves throughout their childhood.³¹³²

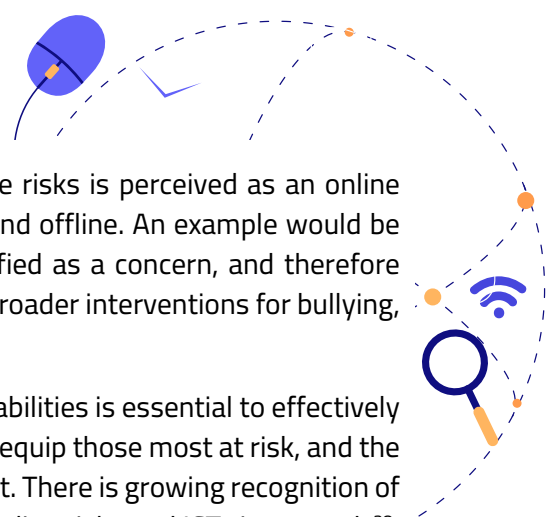
It also moves through different areas of everyday life – homes, schools, communities – and the intersection that online space provides across these physical and social domains. For example, older children are more likely to be exposed to online risks than younger children.³³

Children can also increase their vulnerability by engaging in risky behaviours. Ybarra et al (2006) found that «youth who engage in risky behaviours while online» become vulnerable to the same risks. Thus, those who bully or harass online are more likely to be bullied or harassed as well. This study also demonstrated how the distinction between online and offline can blur, as «one in 4 targets of online harassment report aggressive offline contact from the harasser, such as a phone call or home visit.»³⁴

The results are mixed in terms of sex and risk online. Some studies show that boys and girls are also likely to experience some form of risk related to online bullying. Others show that girls are more likely to be victims of sexual harassment while boys are more likely to be exposed to pornography and graphic images. While boys may be more likely to encounter risks online, girls are more likely to report being in distress as a result of these risks.³⁵³⁶³⁷

As exposure and experience of online risks changes throughout childhood, it's also important to engage with potential changes in vulnerability. A vulnerability lens to address online risks and harms provides a useful framework for identifying where children might be at higher risk or anticipating where the risk could translate into tangible and measurable harm. If, for example, socially isolated children appear to experience higher levels of cyberbullying, educational interventions can be targeted at these children and the capacity of educators, parents and other caregivers to identify and intervene early can be developed.

31 Research Center Innocenti (2011) Child Safety Online: Global Challenges and Strategies. UNICEF p.6
32 Research Center Innocenti (2011) Child Safety Online: Global Challenges and Strategies. UNICEF p. vii
33 Wells et al., 2014; Phyfer et al., 2016
34 Ybarra et al, 2006: 1174.
35 Ybarra et al., 2006
36 Ybarra et al., 2006
37 Phyfer et al., 2016; Livingstone and Hadden, 2009; De Graaf and Vanweesenbeek, (2006).




One of the dangers of this situation is that vulnerability to online risks is perceived as an online vulnerability, rather than a vulnerability in all areas, both online and offline. An example would be in schools or environments where cyberbullying has been identified as a concern, and therefore interventions against cyberbullying are offered independently of broader interventions for bullying, social norms or behavioural change.

Despite this danger, an understanding of online and offline vulnerabilities is essential to effectively target the measures – policies and programmes – that can better equip those most at risk, and the times or places in their lives when these vulnerabilities are greatest. There is growing recognition of the need to better understand how vulnerabilities intersect with online risks and ICTs in general.³⁸

While not exhaustive, an emerging discussion of vulnerabilities based on gender identity and sexual minorities. There is growing evidence that children from minority groups, including LGBT groups, with physical or mental disabilities, or from ethnic minorities are most at risk of being bullied. In a study of Swedish children, bi- or homosexuality was found to be the most important factor in predicting online sexual solicitation. Among 13- to 18-year-olds, those who identified as LGBT were disproportionately at risk of experiencing sexual harassment, particularly online. The same study also showed the transect between online and offline, with sexual harassment most often experienced offline, followed by online harassment.

The increased risk of sexual minority children being victimized online appears to follow the same vulnerability of offline violence. A 2011 study in the United States shows similar results regarding cyberbullying of LGBT groups, with nearly double the number of children identifying as LGBT as heterosexual children reporting being cyberbullied, a result similar to those who were bullied offline. Similarly, a 2013 study in the United States shows that LGBT youth were three times more likely than non-LGBT youth to be bullied or harassed online.³⁹⁴⁰⁴¹⁴²⁴³⁴⁴



While the internet provides a safe space for social interaction for those who may be socially isolated due to, say, their gender identity, so do children with developmental disabilities who may struggle to develop offline relationships and social acceptance. Children with cognitive and developmental disabilities often express an exaggerated desire to make online friendships. Children with autism spectrum disorder (ASD) and Williams syndrome show that the increased vulnerability to offline violence (and especially sexual solicitation) of children with developmental disabilities translates into the online space. Developmental disabilities can work in many ways to increase vulnerabilities, both in the online and offline space. Disorders can be used to increase blind trust and «increased social approach behaviour,» associated with a lower ability to interpret communication signals and the inability to make informed, calculated decisions about who to trust, or that lead to increased social vulnerability. There are also indications that children with other mental health issues, especially depression, tend to seek relationships online and may be more likely to engage with strangers.⁴⁵⁴⁶

38 Livingstone et al, 2017; Wells et al., 2014; Byrne and Burton, 2017; Mitchell et al., 2014,

39 Baek et al., 2014).

40 Suseg and al, 2008).

41 Mitchell, Ybarra and Korchmaros (2014)

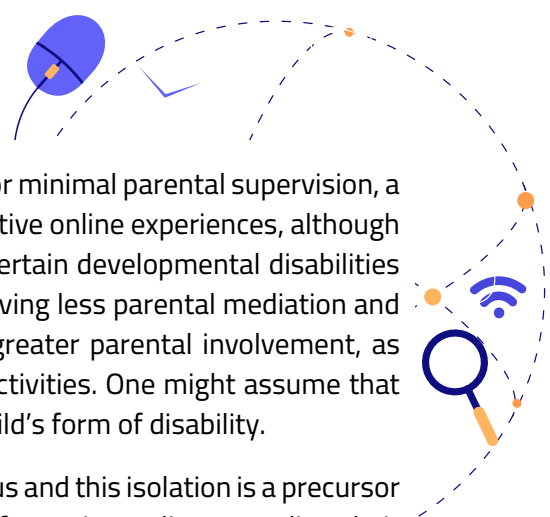
42 Mitchell Ybarra and Korchmaros (2014)

43 Patchin and Hinduja 2011

44 GLSEN et al., 2013.

45 Lough et al., 2015


46 Lough et al. 2015:4



Children with disabilities may also be at higher risk of having little or minimal parental supervision, a factor that has been identified as an important risk factor for negative online experiences, although the evidence for this is varied. For example, while children with certain developmental disabilities (particularly Williams syndrome) are likely to be more at risk of having less parental mediation and attention, children with physical disabilities tend to experience greater parental involvement, as well as greater parental knowledge of their child's⁴⁷⁴⁸⁴⁹⁵⁰ online activities. One might assume that parental attention and involvement may be correlated with the child's form of disability.

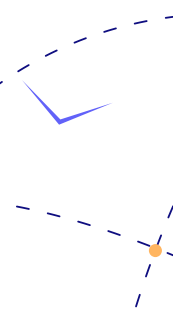
Children often face social isolation as a result of their minority status and this isolation is a precursor to vulnerability. Many children seek refuge, companionship or information online regarding their sexual identity. One of the many benefits of the Internet for minority groups is the use of online spaces for children and young people to explore their sexuality. The support that can be offered through online forums and chat rooms or access to sexual health information has been widely documented.⁵¹

There is growing evidence that LGBT children are much more likely than non-LGBT children to search online for information about health, relationships, sexuality and sexual health. Similarly, online space can help transcend some of the barriers of isolation and communication that children with disabilities may encounter and offer many opportunities, including social or relational, educational or cognitive. The fact that this perceived safe space and supportive environment is then the space used for harassment or bullying can exacerbate the trauma associated with the incident(s) of exclusion, bullying, harassment and other forms of adverse online behaviour.⁵²⁵³



Overall, research suggests that children who are vulnerable or at risk offline are more likely to also be at risk online, worsening cycles of disadvantage and risk. This reinforces the argument that online risks, harms and vulnerabilities are best understood in the literature and broader paradigms of offline risks in children's lives. Education can reduce risky behaviours by raising awareness of the ways in which online choices (for example, contact with strangers) can increase the risk of harm, and also by informing youth about where and how to safely report upsetting experiences.⁵⁴

2. Rights of the child



Children's rights to access the Internet and information and communication technologies (ICTs) are essential to their social and educational development. Thus, restricting or denying Internet access may disadvantage children. In addition, there is substantial evidence that digital skills play an important role in learning, participation and other opportunities for children and young people. The benefits apply offline and also online, «potentially affecting multiple dimensions of children's lives in a digital world.»

47 Fisherman et al., (2012)

48 Livingstone, (2011)

49 Fisher et al. (2012)


50 Whittle et al., 2013

51 For examples, see Boyd, 2014; Gray, 2009; Harpist et al., 2016; Livingstone, 2017, and Boyd et al. 2011 with respect to self-injurious behaviour).

52 GLSEN et al., (2013).

53 SRSF, (2014)

54 Livingstone and Ly.




However, the right to access the Internet also increases the aforementioned risks. In addition, certain inalienable rights enshrined both in the Convention on the Rights of the Child and in other international treaties that Tunisia has ratified, provide a framework for the national, regional and international responses.

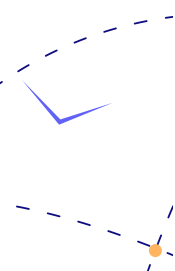
These include children's right to protection from abuse and the rights to justice and redress. In response to legislation and policy in the face of online risks, other children's rights – the right to education, for example – cannot be violated.⁵⁵

2.1. Right to protection against abuse

Due to the hidden nature of online child sexual exploitation and the unregulated environment in which it takes place, policies to protect child ICT users from sexual exploitation must not simply be reactive. The aim should be to prevent abuse before it occurs by strengthening children's ability to protect themselves when using ICTs. This approach is in line with article 19 of the Convention on the Rights of the Child on the right to protection from abuse, which emphasizes the obligation of States to implement, among other measures, educational initiatives to protect children from all forms of violence.⁵⁶



Many parents, schools and other authorities are opting for risk-averse strategies that limit or even prohibit children's access to ICTs. «Most parents struggle with the tension between protecting their children and giving them the freedom to explore, learn and grow independently» (Livingstone & Byrne 2018: 27). The use of «restrictive mediation,» when parents or guardians restrict «screen time,» prohibit or supervise children's online activities, has been one approach. «In middle- and low-income countries, evidence suggests that restrictive mediation is generally favoured by parents, although this entails costs in terms of opportunities for children online, especially girls.» Parents or guardians are also known to remove access to the child's technology assuming that no access will remove the risk, simply restricting access (to the technology or sites and services) is not a sustainable or effective approach to protection.⁵⁷



However, research reveals that restricting internet access is not an effective approach to preventing online risks.⁵⁸ Instead, education (about digital literacy, sexual education, health and relationships) is essential in this regard, as children need information to protect themselves and respond appropriately to the risks they may encounter online. This involves raising their awareness about potential risks so they can identify them, exercise critical judgment and make informed choices. Effective risk prevention depends in part on children's opportunities to build resilience and practice digital citizenship.

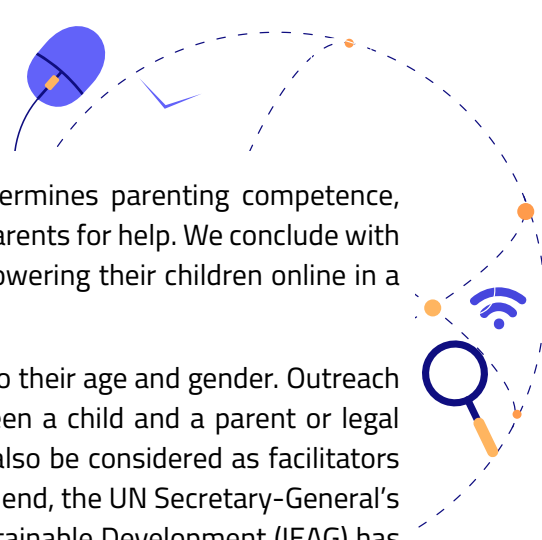
But while awareness and training must be accessible to adults in children's lives (parents, legal guardians, teachers) so that they know the risks and how to protect children, this should not be a substitute for education specifically for children. Notably, children largely seek help or knowledge from their peers rather than their parents, and there have been positive evaluations of mentoring and peer support services.

55 Haddon, L., Cino, D., Doyle, M-A., Livingstone, S., Mascheroni, G., & Stoilova, M. (2020). Digital skills of children and youth: a systematic review of the evidence. KU Leuven, Leuven: ySKILLS p. 8

56 United Nations General Assembly, «Convention on the Rights of the Child», Pub. L. No. Resolution 44/25 (1989), <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>.

57 Livingstone & Byrne (2018) p.19

58 See Kessel, Hardardottir and Tyrefors (2020) <https://www.sciencedirect.com/science/article/abs/pii/S0272775719303966?via%3Dihub>




In all countries, the rapid pace of technological innovation undermines parenting competence, which, in turn, undermines children’s willingness to turn to their parents for help. We conclude with suggestions to help parents meet the growing challenge of empowering their children online in a variety of contexts.⁵⁹

Education must be provided to children in a manner appropriate to their age and gender. Outreach resources that encourage constructive and open dialogue between a child and a parent or legal guardian are also effective. ICTs and online technologies should also be considered as facilitators of child exploitation and, above all, as a tool for protection. To this end, the UN Secretary-General’s Independent Expert Advisory Group on a Data Revolution for Sustainable Development (IEAG) has called for the use of new technologies to support the UN Sustainable Development Goals, in which Goal 16 promotes efforts to end violence and exploitation against children. These are all important considerations in developing an appropriate response to an effective approach to child online protection.⁶⁰

2.2. Access to justice

When children suffer violations of their human rights, including sexual exploitation, they must have access to justice. The UN Committee on the Rights of the Child has stated that «for rights to have meaning, effective remedies must be available to redress violations.» States must therefore «ensure that effective and child-friendly procedures are made available to children and their representatives». This means ensuring that children have meaningful access to the justice system – including «access to a readily available, prompt and effective remedy in the form of criminal, civil, administrative or disciplinary proceedings» – and to any other independent complaints procedure.



To ensure that children’s online safety becomes a reality, several different but complementary approaches are likely to be needed at the national level. This list is not exhaustive but indicative of the complexity of the response required. Ideally, these should not be conceived in isolation from broader (offline) child protection and safety initiatives and approaches, but in relation to these broader issues:

- An appropriate and responsive policy and legislative environment;
- Effective implementation of legislation and policies on the ground in urban and rural areas and across plural legal systems;
- Balance risks and opportunities: find ways to promote healthy and safe engagement while protecting against potentially harmful content, contacts, and behavior;⁶¹
- Sensitize parents, educators and community members to effective protection and prevention;⁶²
- Involvement of industry leaders in safety prevention and consolidation in design;
- Effective detection and tracking systems;

59 Livingstone & Byrne (2018) p.19

60 <https://www.undatarevolution.org/>

61 Smahel et al., «EU Kids Online: Survey Results from 19 Countries.»

62 It is particularly important to address the stigmatization of victims of sexual abuse, by creating a safe space in which children can report abuse and feel safe and receive a positive response and protection.

- Appropriate response and support systems for children.

The International Telecommunication Union (ITU) has outlined five sets of measures to promote children’s online safety. These measures are also largely reflected in the INSPIRE framework:⁶³

- legal measures and remedies;
- technical and procedural procedures;
- organizational structures;
- capacity building; and
- International cooperation.

2.3. Data protection and confidentiality

Personal data is information that can «identify or help identify individuals directly or indirectly in combination with other information» or «any information relating to an identified or identifiable natural person («data subject»)». Therefore, the processing of personal data, for public, institutional or commercial purposes, is a serious concern for the digital privacy of individuals. The extent to which the personal data processed is used, by governments for the purpose of collecting and controlling information or by companies for commercial purposes, is a matter of legal protection.⁶⁴⁶⁵⁶⁶

In particular, «child datafication» is an important issue for online privacy and safety. The European Union’s General Data Protection Regulation (GDPR) of 2018 recognizes children’s right to privacy. It aims to «⁶⁷⁶⁸⁶⁹protect children and their personal data in the digital world» and «seeks to give back a measure of control to the individual (or Internet user) regarding his or her online privacy». He argues that

«Children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards involved and of their rights in relation to the processing of personal data. This specific protection should apply in particular to the use of children’s personal data for marketing purposes or the creation of personality or user profiles and to the collection of personal data concerning children when using services offered directly to a child.»⁷⁰

63 International Telecommunication Union, «ITU Guidelines on Child Online Protection,» 21 May 2021, <https://digitalregulation.org>.

64 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) «Children’s Data and Privacy in line: Growing up in a digital age», London School of Economics and Political Science, London. P.49

65 GDPR – Article 4

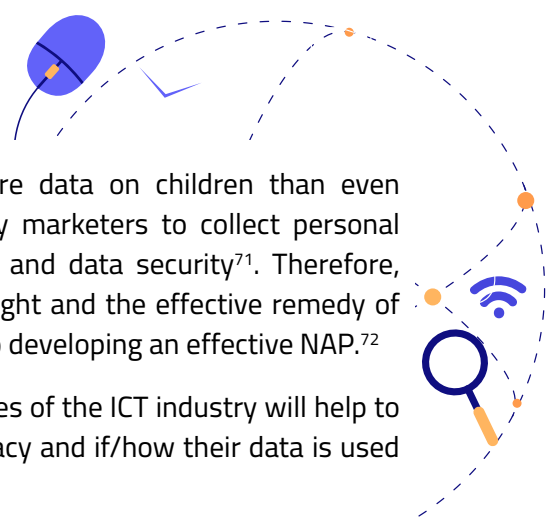
66 «processing» means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR Article 4)

67 «Datafication» refers to the intensified process of surveillance and data collection in which people (including children) are quantified and objectified – positioned as objects (serving the interests of others) rather than subjects (or agents of their own interests and concerns); see Lupton, D. and Williamson, B. (2017) The datafied child: The dataveillance of children and implications for their rights. *New media and society* 19(5), 780-94. De Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) «Children’s Data and Privacy in line: Growing up in a digital age», London School of Economics and Political Science, London.

68 <https://gdpr-info.eu/>

69 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019)

70 Recital 38 GDPR



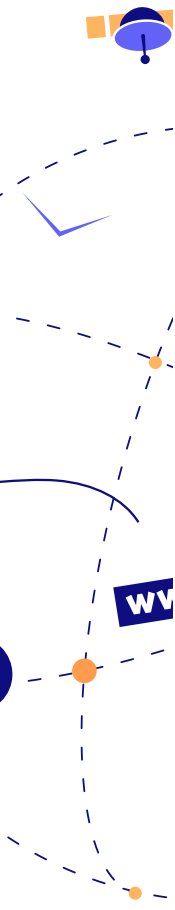
UNICEF acknowledges that commercial companies collect more data on children than even governments do or can collect, while «invasive tactics used by marketers to collect personal information about children have raised concerns about privacy and data security»⁷¹. Therefore, assessing whether Tunisian citizens and minors have both the right and the effective remedy of the protection of personal data and privacy online is paramount to developing an effective NAP.⁷²

Engagement with the Ministry of Home Affairs and representatives of the ICT industry will help to understand the extent to which children benefit from online privacy and if/how their data is used for commercial purposes.⁷³

In addition to institutional and commercial privacy protection, children need to learn how to manage their «interpersonal privacy» regarding their online communication or information sharing. It is often a relational concept, rather than on an individual basis, and is related to what information is shared, when and with whom. It is important to note that this relationship «may be equal or unequal in terms of power and control over the use of personal data.» Therefore, to improve data protection and privacy, digital literacy training and education must help children understand «how information is shared and can be used online both in interpersonal relationships and in business contexts» so that they can benefit from the internet while minimizing risks.⁷⁴⁷⁵⁷⁶⁷⁷

V. International frameworks

As stated above, the technology industry, digital technology and the Internet are global in nature, connected and dependent on relationships, contacts and environments spanning countries, regions and the world. Given this, any attempt to develop strategies or policies to keep children safe online must be situated in contexts and global compacts, and take into account the merging of hyper-local risks and potential harm, as well as the international nature of many forms of risks that children face online and the potential harms that can result.



71 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) «Children's Data and Privacy in line: Growing up in a digital age», London School of Economics and Political Science, London.

72 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) «Children's Data and Privacy in line: Growing up in a digital age», London School of Economics and Political Science, London.

73 control Individual on Information Disclosure and Visibility Ghosh, A.K., Badillo-Urquiola, K., Guha, S., et al. (2018) Safety vs. surveillance: What children have to say about mobile apps for parental control. Conference on Human Factors in Computer Systems. Montreal Canada: GFA, 1-14.

74 Hargreaves, S. (2017) Relational privacy and crime. *William and Mary Journal of Women and the Law* 23(3), 433-76.

75 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London. P49

76 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London. P49

77 Council of Europe. (2020) Handbook for Policymakers on Children's Rights in the Digital Environment: <https://rm.coe.int/publication-it-handbook-for-policy-makers-on-the-rights-of-the-child-f/1680a0ae2c>

1. International conventions applicable to Tunisia

The safety and well-being of children online cannot be separated from the broader rights that children do not enjoy. The safety of children is based on the rights of all children, enshrined in the Convention on the Rights of the Child, to protection from harm (Article 19). It is therefore impossible to talk about the protection of children from online child sexual exploitation and abuse (78EASEL) and all forms of violence facilitated by technology, let alone the collective and indivisible rights of children.⁷⁹

The growing importance of the internet and technology in children's lives, and the opportunities they present, mean that when we ensure that children are protected online, the opportunities that the digital world offers children are not diminished. The rights of all children are enshrined in the United Nations Convention on the Rights of the Child (CRC), to which Tunisia (as well as all but two countries in the world) are parties. The CRC identifies all the rights to which children are entitled and which must be protected by UN Member States, ranging from the right to privacy, protection and education, to the right to housing, education and health care.⁸⁰

Just as children have the right to be safe offline, they have the right to education, water, sanitation and health care, and these rights must not be compromised by measures taken to keep children safe. The right to education, for example, cannot come at the expense of security, if schools are not safe. Similarly, the right to education cannot be compromised to guarantee a child's right to safety and a safe life. The same applies online. The right to be safe online cannot come at the expense of the rights to education, information or healthcare, for example, which children can increasingly access online. Similarly, research from around the world has shown that when children are not safe online, they are not able to fully realize the benefits that exist for them through the internet and technology.⁸¹



General comment No. 25 requires States (inter alia) to take measures, including through the development, monitoring, implementation and evaluation of legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent the use of their online networks or services in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and guardians with prompt and effective remedies.

Until recently, the lack of evidence on what works to keep children safe online has led to approaches to online safety that restrict children and young people's access to technology and the internet. Today, a growing body of research and evidence allows us to better understand how to protect children's opportunities and rights online, while keeping them safe.


In January 2021, the CRC took a landmark decision in its adoption of General Comment 25 (GC.25), noting that all children's rights apply equally online as offline, and that there should be no distinction between the digital and offline environment. It is important to note that the General Comment also provides guidance to all States parties to the CRC on the realization of children's rights in the

78 United Nations Committee on the Rights of the Child. (1989). Convention on the Rights of the Child. General Assembly resolution 44/25, 20 November 1989.

79 Livingstone Sonia; Byrne, Jasmina; Carr, John (2016). One in three: internet governance and children's rights, Innocenti working papers, No. 2016-01, UNICEF Research Office - InnocentiFlorence

80 United Nations Committee on the Rights of the Child. (1989). Convention on the Rights of the Child.

81 To see by example, Kardefelt Winther, Daniel; Livingstone, Sonia; Saeed, Mariam (2019). Growing up in a connected world, Innocenti Research Report, UNICEF Research Office - InnocentiFlorence



digital environment. Thus, the need to balance the right to online security and protection with the opportunities that arise is enshrined in the interpretation of the Convention on the Rights of the Child. GC.25 and which also sets out four cross-cutting principles that are essential for the realization of children's rights in the digital environment: non-discrimination, the best interests of the child, the right to life, survival and development; and respect for the views of the child.⁸²

These principles have a direct impact on all aspects of products and services offered by the technology industry and the private sector:

- they must take into account how these products and services benefit all children, including children with disabilities; those who may not be able to afford services and are therefore significantly disadvantaged in the realization of other rights, such as education; or those who may live in rural areas (to name but a few);
- they must always consider whether products and services, particularly those targeting children, are likely to be in the best interests of the child, or whether they may pose risks and harm the best interests of the child;
- they must assess whether the products or services they provide compromise or threaten the life, survival or well-being of the child, or may have a substantial impact on the child's development (this includes products that may introduce risks into children's lives that may have a negative impact on cognitive development outcomes, health or educational); and⁸³
- They need to consider what children themselves think, experience and express about their experiences of products and services, as they are better suited to reflect their own experiences, rather than having those experiences and opinions imposed on them by adults.




Finally, GC.25 calls on Member States – all those that have signed and ratified the Convention on the Rights of the Child – to ensure that the private sector exercises due diligence on the impact of their products and services on children's rights, and to take measures to monitor, prevent and act against companies and others that violate children's rights as set out in the Convention.⁸⁴

This explicitly places a responsibility on all technology and telecommunications industries to ensure that their products are safe for children, while protecting all competing rights of the child. These include the right to harm protection, information, participation and education, in and through the products and services they develop and provide. In addition, it is the responsibility of the State to ensure that this happens and to take action when companies violate children's rights. It also identifies the role of the State in ensuring that measures to protect children online are taken in all places where children could access the internet, ranging from schools, internet cafes, other public access points and at homes. It draws attention to the role of the wider child protection system, noting that online protection should be integrated as far as possible into a broader protection and case management system.

⁸² United Nations Committee on the Rights of the Child. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment. CEC/C/GC/25. March 2, 2021.

⁸³ A useful operationalization of risks, such as content, conduct, contract, and contact risks, can be found here: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Online Risk Classification for Children. (Series of CO:RE short reports on key topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>

⁸⁴ United Nations Committee on the Rights of the Child, 2021




Noting the intersection between online and offline risks, the General Comment also calls on States to implement measures to help parents and guardians best manage children's device and internet use, as well as broader parenting measures that promote positive communication, support, empathy and other critical life skills.

In addition to the CRC and subsequent General Comments, Tunisia is also a signatory, without reservation, to the Optional Protocol to the CRC on the sale of children, child prostitution and child pornography (OPSC). Tunisia is also the only MENA State to have ratified the Council of Europe

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (in force since 2010), known as the Lanzarote Convention, and is also a signatory (although it has not fully acceded to) the Convention on Cybercrime, better known as the Budapest Convention. Although the Lanzarote Convention was formulated before awareness of the potential impact of the digital environment on the sexual abuse and exploitation of children, it remains the first international treaty that addresses the sexual abuse of children within the family and the sexual exploitation of children in tourism and travel. Its provisions also extend to the digital environment, and it remains one of the most important and legally binding global child protection mechanisms. Specifically, Article 18 provides for the criminalization and prevention of sexual abuse of children, Article 19 applies to the sale of children in child prostitution, Articles 20 and 21 deal with child pornography and Article 23 of the Lanzarote Convention deals with the solicitation of children for sexual purposes. The Budapest Convention (in force in 2016) directly addresses the sexual abuse and exploitation of children online and, Article 9 of the Convention, directly addresses the prohibition of child pornography.⁸⁵

2. Global Frameworks for Online Safety



Several frameworks, strategies and guidance exist at the global level to help countries develop prevention and response strategies to address all forms of online violence against children, as well as more targeted guidance on online child sexual exploitation. These range from national strategies such as the INSPIRE Strategies to End Violence against Children (INSPIRE) and the National Response Model (NRM), developed by the WeProtect Global Alliance to Combat EASEL. Linked to these are industry-specific recommendations, which offers protocols and specific assistance to identified stakeholders, in which more detailed actions, directly relevant to their operational context, can be formulated by each of these different stakeholders to prevent and respond to all forms of online violence against children. Examples of these include ITU guidelines for industry/parents/schools on child online protection. This section outlines each of them relevant to the technology industry, and how they can be adapted to the Tunisian context.

⁸⁵ Note that the Lanzarote and Budapest Conventions were formulated before the recognition of the need to change language to better reflect the abusive nature of the use and depiction of children in pornography, and therefore the original texts still refer to the term child pornography, rather than the more recent terminology, following the guidelines of the CRC, Child Sexual Exploitation Material (PESC).

2.1. INSPIRE Strategies: Seven Strategies to End Violence Against Children.

The INSPIRE Strategies are seven evidence-based strategies to end violence against children, developed by the World Health Organization, UNICEF and other international agencies. These strategies focus on seven areas:

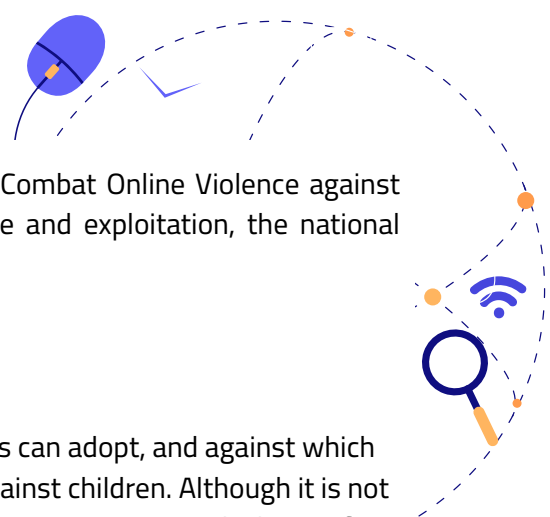
1. implementation and enforcement of laws,
2. standards and values,
3. safe environments
4. support for parents and caregivers,
5. income and economic strengthening,
6. intervention and assistance services, and
7. education and life skills.

Essentially, global evidence shows that investment in each of these areas yields positive results in reducing violence against children. Although these strategies have been tested and developed to address all forms of violence against children, without focusing specifically on online protection or violence experienced by children in the online space, they each have a direct impact on the forms of violence experienced online and the steps that can be taken to both prevent and respond to online violence against children.

INSPIRE clearly reflects the need for an intersectoral and whole-of-society response to prevent violence against children in all its forms. While national law enforcement and criminal justice capacity of the State is necessary, within a sound policy and legislative environment, to investigate and prosecute crimes against children, the child protection system, education and health, as well as non-State actors within civil society, and the technology industry, must actively participate in creating non-violent normative environments, supporting parents and caregivers, providing intervention and support services, and providing comprehensive life and health education.

INSPIRE has relied on evidence of the importance of providing safe physical environments for children. This can result in the creation and promotion of secure digital environments, an outcome in which industry and government have a critical role to play. The tech industry has an obligation to provide and promote safe digital environments for children – digital spaces, apps, games and services that take into account children's needs and rights from the outset, from the conceptualisation and design of the service or product itself. This consideration of the potential impact on children can be institutionalized through the adoption of tools such as child rights impact assessments and principles of safety (and confidentiality) by design.

INSPIRE strategies are important for Tunisia. It is important that any action to combat violence against children takes into account all forms of online violence against children, especially given the continuum and intersection between online and offline violence. Conversely, all measures or actions taken to tackle online violence are firmly anchored in the broader strategy to end violence against children, to ensure the integration of services and responses.




These actions are reflected in the Second Global Framework to Combat Online Violence against Children, and more specifically against online child sexual abuse and exploitation, the national response model.


2.2. The National Response Model

The National Response Model is a model framework that countries can adopt, and against which they can measure their strategies in addressing online violence against children. Although it is not based on specific evidence, it proposes different thematic areas or «capacities» in which specific activities at national and local levels can be adapted to produce targeted positive outcomes for children. These include:

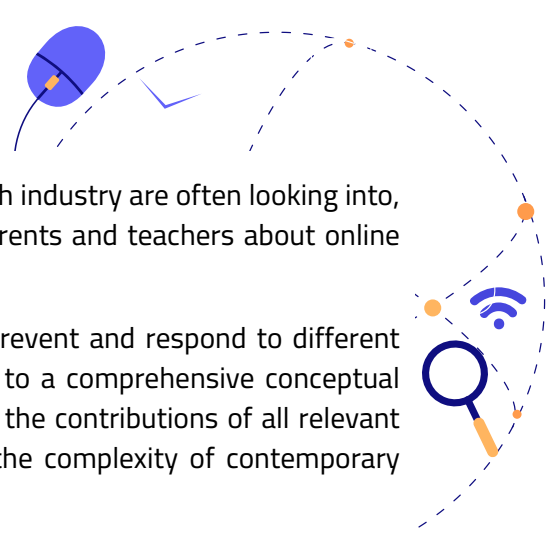
1. Policy and legislation
2. Criminal justice
3. Victim
4. Societal
5. Industry
6. Media and communication

Similar to the INSPIRE strategies, the NRM provides a tool for countries to address online violence against children. The NRM covers all aspects of society, but has a specific industry-focused capacity and its role in preventing and responding to online violence. Specifically, industry capacity requires a country's technology industry to:

- 
- Act on notification and withdrawal procedures,
 - be governed by statutory protections that allow industry to fully and effectively report the SEME, including its transmission, to the designated (enforcement) agency,
 - Engage in the development of innovative solutions to help address local problems of online violence, and
 - Engage in effective child-centred corporate social responsibility.



An important dimension of MNR is its focus on effective leadership and coordination of different individual focus areas involved in addressing ICT-related violence and abuse. Whereas previously interventions to address ICT-related violence and abuse focused on response and support systems, e.g. through hotlines and helplines to report abuse and targeted support to victims, etc., the NRM takes a broader societal perspective. This follows a trend reflected in other public health approaches towards primary and secondary strategies to prevent or reduce the incidence of harm by targeting policies and interventions to known risk indicators, identifying and responding to problems as they arise, and minimizing the long-term effects of harms.



This is an area that governments and the private sector of the tech industry are often looking into, supporting awareness campaigns and messages for children, parents and teachers about online safety, thereby raising awareness of potential risks online.⁸⁶

Individually, INSPIRE and the NRM address specific actions to prevent and respond to different aspects of violence against children. Combined, they contribute to a comprehensive conceptual framework for policy and programmatic responses that draw on the contributions of all relevant actors within an appropriate ecological framework and reflect the complexity of contemporary socio-technological environments.

2.3. Global guidelines for the digital industry

In addition to the imperative to comply with the above frameworks, there are several industry-specific frameworks and guidelines to help the tech industry, from social media companies to mobile operators, developers, fintech, or content creators, achieve these outcomes. This can lead to a successful balance between children's right to protection from online harm and their right to privacy, information and participation. These include ITU COP guidelines, children's rights and the Global Children's Forum Business Principles and Child Rights Self-Assessments.

ITU Guidelines on Child Online Protection:

The International Telecommunication Union (ITU), in collaboration with UNICEF, has developed specific guidelines for the technology industry (as well as for teachers and parents), taking a child rights-based approach, which provides a roadmap for the private technology industry to ensure and promote online protection. It is important to note that these are not general guidelines, but are targeted at the needs and operations of the technology and telecommunications industry, as well as parents and teachers, respectively.



These guidelines outline five specific areas where industry can protect and promote children's rights to ensure the safety and protection of children:

1. **Integrate children's rights into all appropriate corporate policies and management processes.** This requires reviewing each company's internal policies and processes to ensure that the best interests of children are at the centre of decisions, and that all internal processes are established to protect the well-being and rights of children, and to act internally and responsibly, when these rights are compromised or violated.
2. **Develop standard processes for managing child sexual exploitation (HEM) material.** Child sexual exploitation material is now primarily housed, transmitted, shared and produced using digital technology. Every company, regardless of the service or products it provides, must have internal and external policies and protocols in place to detect, identify, return, and remove MESE material from the company's networks, URLs, services, or products, as well as to collaborate with national and international legislation, law enforcement, and civil society in addressing the MESE.
3. **Create a safer and age-appropriate online environment.** Products and services provided by the private sector must always take into account the different risks children face

⁸⁶ World Health Organization. (2006). Child Abuse Prevention Guide: Intervention and Data Generation: https://apps.who.int/iris/bitstream/handle/10665/43686/9789242594362_fre.pdf?sequence=1souteni

online – content, contact, conduct and contract – and take the necessary steps to create products that are «easy to use, safe and private by design and privacy» that are age-appropriate for all users, including children.⁸⁷

4. Educate children, caregivers and educators about child safety online and responsible use of ICTs. While companies play a vital role in ensuring that children's online experiences and their use of technology are safe, parents, teachers and other responsible adults in children's lives also play an important role in promoting the skills children need to stay safe by taking specific age-appropriate measures. Companies therefore have an important role to play in educating and empowering parents and teachers in their role of keeping children safe, in how and what are the limitations of tools such as parental monitoring tools, and what is the appropriate use of technology and online activities at different ages and stages of child development.
5. Promote digital technology as a way to increase civic engagement. Article 13 of the Convention on the Rights of the Child enshrines the right of children to expression and participation through all means of their choice. This is also reflected in GC.25 which notes the responsibilities of States to protect children's right to participation and expression, including through the use of digital technology and the Internet. It is important for companies to ensure that the products and services they develop, and the measures they take to protect children online, do not infringe on the right of these same children to express themselves through technology and the Internet, or to participate in the wealth of activities and opportunities that being online offers. Equally important, businesses can invest in promoting children's participation, as well as the skills required to participate equitably in civic life.

It is important to note that the ITU Guidelines for Policymakers on Child Online Protection (COP) are a comprehensive report based on the Convention on the Rights of the Child and the United Nations Sustainable Development Goals. This research draws on the report's recommendations, strategies, and best practice examples to inform both the research design and the key research deliverable: a national action plan for Tunisia.⁸⁸

The ITU report argues that in a national COP plan, children's rights to Internet access must be balanced with 1) protection mechanisms, such as industry regulation, a legal framework, law implementation and 2) skills development in the form of online safety education.⁸⁹

«Children must not only have access to the internet, but also be protected from online harm, and have the digital citizenship skills to manage online risks and threats.»⁹⁰


The report emphasizes the need for national coordination when creating COP plans and includes approaches on how to design an inclusive, «coordinated and cooperative multi-stakeholder national strategy».

⁸⁷ International telecommunications industry. (2020). p 8

⁸⁸ <https://www.itu-cop-guidelines.com/policymakers>

⁸⁹ An overview of existing educational frameworks can be found at Cortesi, Sandra, Alexa Hasse, Andres Lombana-Bermuda, Sonia Kim and Urs Gasser. 2020. Youth and Digital Citizenship+ (More): Understanding skills for a digital world. Berkman Klein Center for Internet and Society

⁹⁰ ITU (2020b) Keeping children safe in the environment digital: The importance of protection and empowerment – Guidance note. P.3




«The protection of children and young people is a shared responsibility and policymakers, industry, parents, caregivers, educators and other stakeholders must ensure a sustainable future where children and young people can thrive and fulfill their potential – online and offline – and where they can be guaranteed a safe and empowering digital environment.»⁹¹

An effective national strategy, however, must include input from relevant stakeholders, namely «children and their parents, caregivers and guardians», while the responsibilities of the private sector towards children’s rights must not be neglected. The report highlights the need to include children’s perspectives. It calls for «open consultations and dialogues with children, to develop better targeted measures and more effective actions» and to ensure that the needs of vulnerable groups are not excluded.⁹²⁹³

It stresses the importance of legal reform, the development of new policies or the integration of existing ones, as «international human rights standards (such as the Convention on the Rights of the Child and its Optional Protocols)» must be harmonized with national laws.⁹⁴

Overall, it presents an ideal course of action as an inclusive process with defined roles and responsibilities for key stakeholders, namely ministries, law enforcement, health and social service organisations, the ICT industry, civil society, children and their parents/guardians, and the academic and research community. In addition, it advocates a holistic vision of reform in which policy changes should be addressed in the areas of children’s rights, legislation, law enforcement, regulation, monitoring and evaluation, the ICT industry, reporting, social services and victim support, data collection and research, education, and national awareness and capacity.⁹⁵

Children’s rights and the business principles of the Global Compact



In addition to the above, guidance such as the Global Compact’s Principles on the Rights of the Child and Business (CRBP) provides a useful framework for Tunisia to examine the role and responsibilities of the tech industry in protecting children and ensuring that children’s collective rights are protected.

The CRBP, developed by the Global Compact, UNICEF and Save the Children, identifies ten principles that companies must adhere to to ensure children’s rights are respected. Businesses must:

1. Fulfill their responsibilities to respect children’s rights and commit to supporting children’s human rights;
2. Contribute to the elimination of child labour in all business activities and practices;
3. Provide decent work for young workers, parents and caregivers;
4. Ensure the protection and safety of all children in all commercial activities and facilities;

⁹¹ ITU (2020b) Keeping children safe in the environment digital: The importance of protection and empowerment – Guidance note. P

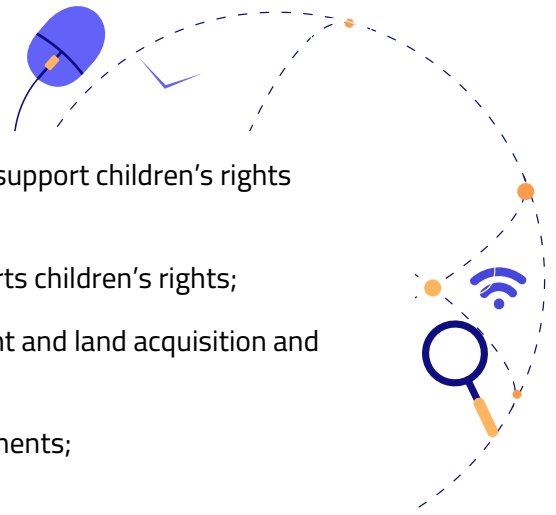
⁹² ITU (2020b) Keeping children safe in the environment digital: The importance of protection and empowerment – Guidance note. P.3

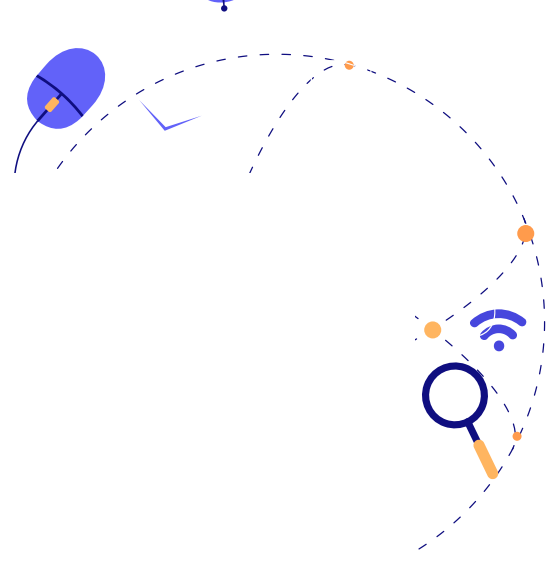
⁹³ ITU (2020a) Guidelines for policymakers on child online protection. p. vi

⁹⁴ ITU (2020b) Keeping children safe in the environment digital: The importance of protection and empowerment – Guidance note. P.3

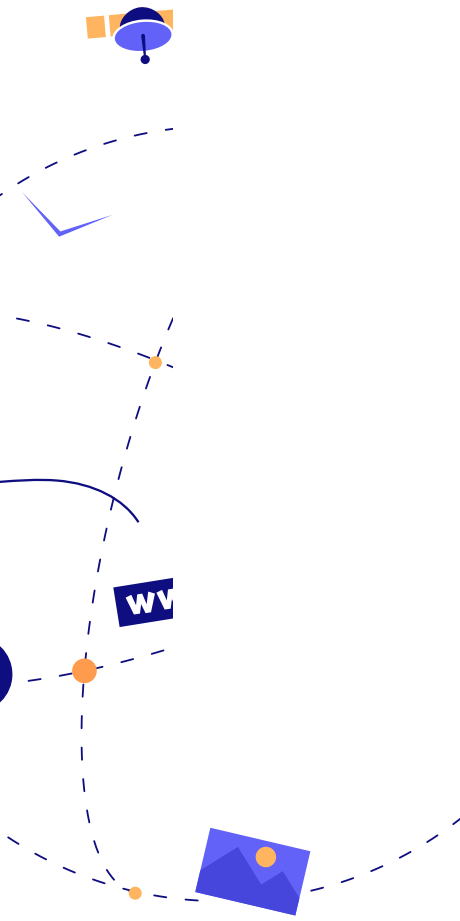
⁹⁵ ITU (2020b) Keeping children safe in the environment digital: The importance of protection and empowerment – Guidance note. pp.5-7

5. Ensure that products and services are safe and seek to support children's rights through them;
6. Use marketing and advertising that respects and supports children's rights;
7. Respect and support children's rights to the environment and land acquisition and use;
8. Respect and support children's rights in safety arrangements;
9. Help protect children affected by emergencies;
10. Strengthen community and government efforts to support and protect children's rights.





Annex 2: Mapping of the legal and institutional framework for online child protection in Tunisia



I. The legal framework for online child protection in Tunisia

The mapping of the Tunisian legal framework has demonstrated the existence of several legislative texts that address the issue of online violence against children, directly or indirectly. These texts address the issue from different angles of a sectoral nature. Indeed, there is currently no legal text that addresses the issue in a holistic way linking childhood and online violence. For example, the provisions on violence against children online are scattered across several texts. The types of child maltreatment can be classified into two broad categories:

- attacks on the physical integrity of children;
- attacks on their human dignity.

The legal texts governing the matter are as follows:

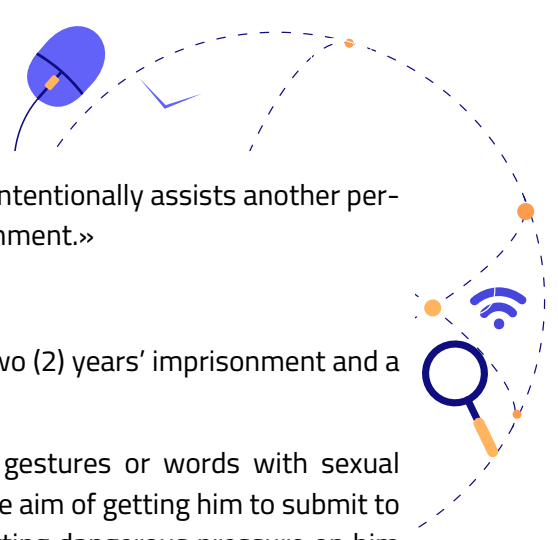
- Texts relating to violence against children (the Criminal Code, the Child Protection Code, Organic Law No. 58 - 2017 of 22 August 22, 2017 on the elimination of violence against women, Organic Law No. 61 of 2016 of August 3, 2016 on preventing and combating trafficking in persons, Organic Law No. 26 of 2015 of August 7, 2015 on combating terrorism and preventing money laundering);
- Texts relating to information/communication (Article 2001-01 of January 15, 2001 promulgating the Telecommunications Code, Law 2004-63 of 27 July 27, 2004 protection of personal data, Decree-Law No. 115 - 2011 of November 2, 2011 on freedom of the press, Decree-Law No. 2022-54 of September 13, 2022, on the fight against crimes relating to information and communication systems).

1. Physical and moral integrity in the 2022 Constitution

The Tunisian legislature elevated the right to dignity to constitutional status in Article 25 of the new Constitution of the Republic of Tunisia, which stipulates that «the State shall protect the dignity of the human person and the sanctity of the body, and prohibits morals and physical. This protection is attested to by several previous legislations. Thus, Article 24 of the Constitution considers that the right to life is a sacred right and that it is not permissible to infringe it except in extreme cases laid down by law. Article 30 states: «The State shall protect privacy, the sanctity of the home and the confidentiality of correspondence, communications and personal data. Similarly, Article 38 enshrines the right of access to communication networks.

2. Cyberviolence and electronic crimes in the penal code

The concept of electronic crime was first introduced into the Criminal Code in 1999 by Article No. 89 of August 2, 1999 amending and supplementing certain provisions of the Criminal Code. Articles 172, 199 bis and 199 ter now enshrine the offence of information and criminalize acts of perjury that may result from the use of new information and communication technologies.



Article 206 of the Criminal Code stipulates that «any person who intentionally assists another person in committing suicide shall be punished by five years' imprisonment.»

Article 226 ter (new) states that

«Anyone who commits sexual harassment shall be punished by two (2) years' imprisonment and a fine of five (5) thousand dinars.


Sexual harassment is any assault on another person by acts, gestures or words with sexual connotations that violate his dignity or affect his modesty, with the aim of getting him to submit to the sexual desires of the aggressor or those of others, or by exerting dangerous pressure on him likely to weaken his ability to resist it. »

The penalty is doubled if:

- the victim is a child,
- the perpetrator is an ascendant or descendant of the victim, whatever the degree,
- the perpetrator has authority over the victim or abuses the authority conferred on him by his or her duties,
- The offence committed is facilitated by the apparent situation of vulnerability of the victim, or known to the perpetrator.

The limitation period for criminal proceedings concerning the offence of sexual harassment committed against a child is effective from the time of reaching the age of majority.

It is clear from this Article that harassment can be perpetrated by other modern means of communication through the sending of images and other means in order to induce others to respond to sexual desires and to put pressure on them.



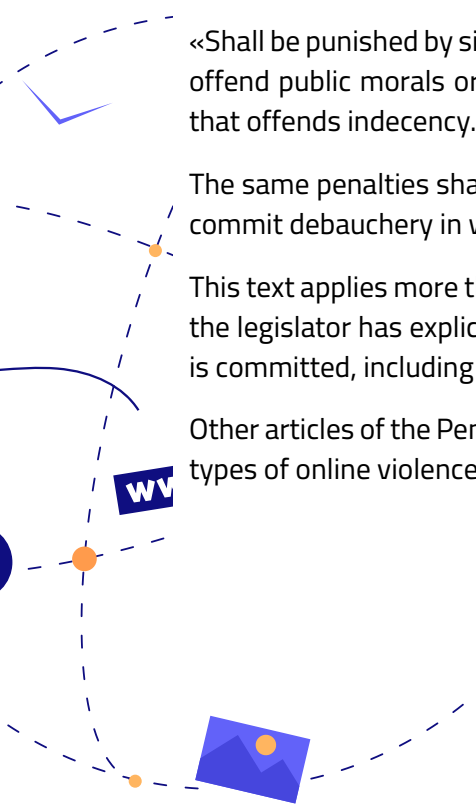
In addition, Article 226 bis, after its revision in accordance with Article 2004-73 of August 2, 2004, stipulates that:

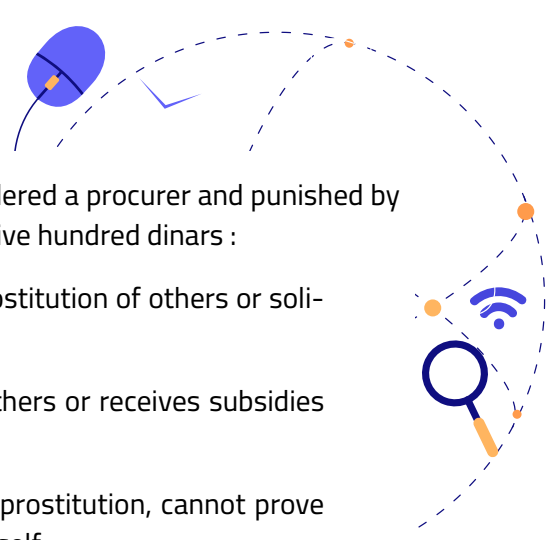
«Shall be punished by six months' imprisonment and a fine of one thousand dinars that may publicly offend public morals or morals by the gesture or word or intentionally annoy others in a manner that offends indecency.

The same penalties shall be imposed on anyone who publicly draws attention to an opportunity to commit debauchery in writings, recordings, audio or visual, electronic or optical messages. »

This text applies more than any other to all pornographic works disseminated via the Internet, since the legislator has explicitly mentioned the electronic means by which any offence against morality is committed, including mediation in prostitution and pornography disseminated on the network.

Other articles of the Penal Code, including Articles 232, 233, 234 and 235, are applicable to different types of online violence.






Article 232 of the Criminal Code stipulates that he or she is considered a procurer and punished by imprisonment of one to three years and a fine of one hundred to five hundred dinars :

1. who, in any way, knowingly aids, protects or assists the prostitution of others or soliciting for prostitution;
2. who, in any form, shares the proceeds of prostitution of others or receives subsidies from a person habitually engaged in prostitution;
3. who, knowingly living with a person habitually engaged in prostitution, cannot prove sufficient resources to enable him to support himself or herself;
4. who hires, induces or maintains, even with his consent, a person of full age, with a view to prostitution, or delivers him to prostitution or debauchery;
5. acts as an intermediary, in any capacity, between persons engaged in prostitution or debauchery and individuals who exploit or remunerate the prostitution or debauchery of others.

Attempt is punishable. »

Article 233: «The penalty shall be imprisonment for three to five years and a fine of five hundred to one thousand dinars in cases where:

1. the offence was committed against a minor;
 2. the offence was accompanied by coercion, abuse of authority or fraud;
 3. the offender is carrying an apparent or hidden weapon;
 4. The offender is the spouse, ascendant or guardian of the victim or had authority over him or if he is his servant for hire or if he is a teacher civil servant or minister of religion or if he has been assisted by one or more persons. »
- 

Article 234: « Subject to the heavier penalties provided for in the preceding article, any person who offends morals by exciting, promoting or facilitating the debauchery or corruption of minors of either sex shall be punished by one to three years' imprisonment and a fine of one to five hundred dinars. »

Article 235: « The penalties provided for in Articles 232, 233 and 234 above shall be imposed even though the various acts which constitute the constituent elements of the offences have been carried out in different countries. The guilty of the offences referred to in the above-mentioned articles shall, by judgment, be placed in a state of residence ban for not more than two years. »

3. Article 2001- 01 of January 15, 2001 promulgating the Telecommunications Code

The legislator has sought the organization of the telecommunications sector, and the creation of a national telecommunications authority.

Article 86 of the Telecommunications Code provides that «Anyone who knowingly harms third parties or disturbs their peace through public telecommunications networks shall be punished by imprisonment of one (1) year to two (2) years and a fine of one hundred (100) to one thousand (1000) dinars.»

4. Organic Law No. 26 of August 7, 2015 on Combating Terrorism and Preventing Money Laundering

Article 5 stipulates that «anyone who is guilty of terrorist offences under this Article and shall be liable to half of the penalties relating thereto:

- inciting by any means to commit them, provided that this act generates, by its nature or context, a possible danger of their commission.
- resolving to commit them, if this resolution is accompanied by any preparatory act for its execution.

If the penalty is death penalty or life imprisonment, it shall be replaced by imprisonment for twenty years. »



The development of information systems has led to the emergence of new forms of organized crime, including electronic terrorism, which depends on the use of scientific and technological capabilities to intimidate and harm others. The terms of that article cover this kind of infringement made via the internet.

5. Decree Law No. 115 - 2011 of November 2, 2011 on Freedom of the Press

Article 50 of this decree stipulates that:

«Those who directly incite an individual or several individuals to commit the said act, if the incitement has been effective, shall be punished as accomplices to an act classified as an offence, according to the definitions laid down in Article 51 et seq. of this Decree-Law, if the incitement has been followed by effect, by means of speeches, words, threats in public places, by means of posters and announcements displayed to the public or by any means of audiovisual and electronic information, shall be punished, as accomplices to an act classified as an offence, in accordance with the definitions laid down in Article 51 et seq. of this Decree-Law, attempted offences are punishable in accordance with the provisions of Article 59 of the Criminal Code.¹»

However, the criminal provisions included in the Terrorism Act and Decree Law 115 are not sufficient to criminalize incitement to murder via the Internet. These laws are considered specific provisions setting out their own scope in these laws and are insufficient to combat all other forms of incitement to murder online. There is a need for a comprehensive law criminalizing incitement to murder via the Internet. However, the legislature did not specify the means chosen for this purpose, but stipulated that these must be intentional assistance, that is, the need to establish the element of criminal intent in this crime.

In this context, it is necessary to expose oneself to the game of the «blue whale» or the «Blue whale challenge» which is an online game composed of challenges for fifty days and in the last challenge the game asks the player to commit suicide. This game started in Russia in 2013 with the social network «Vkontakte» and caused the first suicide in 2015.

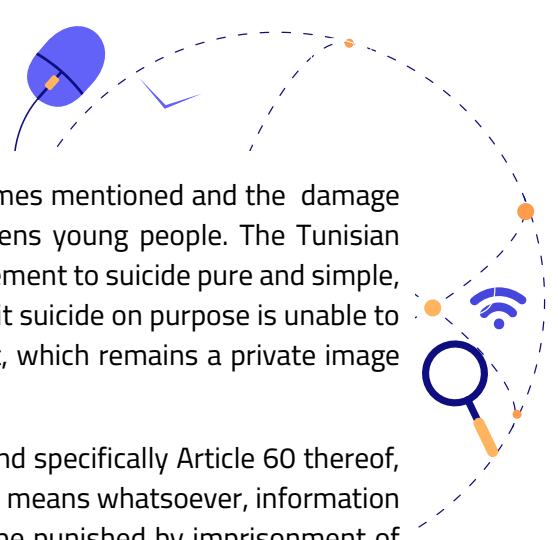


An emergency judgment number 54909 was rendered by the Court of First Instance of Sousse on March 5, 2018 which ordered the Tunisian Internet Agency, in the person of its legal representative, to block the game «blue whale» and Mariam's game from all websites, social networks and application stores and download links accessible on the Tunisian Internet.

He came up with the court's reasoning:

in view of Article 46, second paragraph, of the Child Protection Code, that any positive or negative action that threatens the life of the child or his or her physical or moral integrity in a manner that cannot be remedied is considered an imminent danger. And where there is no doubt that such dangerous games have a direct violation of the child's right to life guaranteed by Article 22 of the Constitution, Article 6 of the International Convention on the Rights of the Child and Article 22 of the Child Protection Code, which protect him or her from all forms of violence, of ill-treatment and physical abuse, which requires urgent judicial intervention to protect the child's right to life and physical integrity, according to the provisions of Article 201 of the CCPC, and what is recognized by the Constitution in Article 42.

¹ Article 51 criminalizes incitement to "committing a crime of homicide, bodily harm, rape or pillage»



The judge is summoned in view of the seriousness of the two games mentioned and the damage of the imminent use of it and the imminent danger that threatens young people. The Tunisian legislator has not subjected the Penal Code to the offense of incitement to suicide pure and simple, Article 206 which criminalizes the act of helping others to commit suicide on purpose is unable to encompass the situation of incitement to suicide via the Internet, which remains a private image and requires the promulgation of a special text.

We can also mention Decree-Law 115 on freedom of the press and specifically Article 60 thereof, which stipulates that «anyone who intentionally transmits, by any means whatsoever, information relating to crimes of rape or sexual harassment of minors, shall be punished by imprisonment of one to three years and a fine of three thousand to five thousand dinars, mention the name of the victim or disclose any information that may lead to the victim's knowledge.

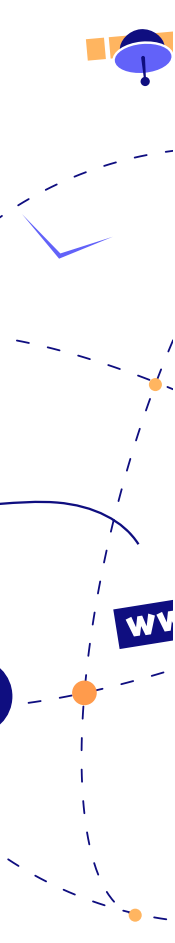
The same penalty shall be imposed on anyone who knowingly provides, distributes, exports, produces, publishes, exhibits, sells or possesses child pornography. »

6. Organic Law No. 58-2017 of August 22, 2017 on the Elimination of Violence against Women

Article 3 defines violence against women as:

«Any physical, moral, sexual or economic harm to women based on discrimination based on sex which results in bodily, psychological, sexual or economic harm, suffering or injury to women, including the threat of such harm, pressure or deprivation of rights and freedoms, whether in public or private life.»

The same Article defines the types of violence against women as follows:

- 
- «Physical violence: any harmful act or abuse affecting the physical integrity or safety of the woman or her life, such as beatings, kicks, injuries, pushing, disfigurement, burns, mutilation of parts of the body, forcible confinement, torture and homicide,
 - Moral violence: any verbal aggression, such as defamation, insult, coercion, threat, abandonment, deprivation of rights and freedoms, humiliation, neglect, mockery, belittling and other acts or words that violate the human dignity of women or are intended to intimidate or dominate them,
 - Sexual violence: any act or word intended by the perpetrator to subject the woman to her own sexual desires or to the sexual desires of others, by means of coercion, fraud, pressure or other means, likely to weaken or interfere with the will, regardless of the relationship of the perpetrator with the victim,
 - Political violence: any act or practice based on gender discrimination the perpetrator of which is intended to deprive or prevent women from engaging in any political, partisan, associative activity or any fundamental right or freedom,

- Economic violence: any act or failure to exploit women or deprive them of economic resources, regardless of their origin, such as deprivation of funds, wages or income, control of wages or incomes and prohibition of work or coercion to work,
- Discrimination against women: any distinction, exclusion or restriction which has the effect or purpose of impairing or impairing the recognition of women's human rights and freedoms, on a basis of full and effective equality, in the civil, political, economic, social and cultural fields, or of impairing such recognition or the enjoyment or exercise of these rights by women, regardless of colour, race, religion, thought, age, nationality, economic and social conditions, marital status, state of health, language or disability. »

7. Organic Law No. 61 of 2016 of August 3, 2016 on Preventing and Combating Trafficking in Persons

Article 1 of the Act stipulates that:

«The purpose of this Law is to prevent all forms of exploitation to which persons, in particular women and children, may be exposed, to combat their trafficking, to punish the perpetrators and to protect and assist victims. »

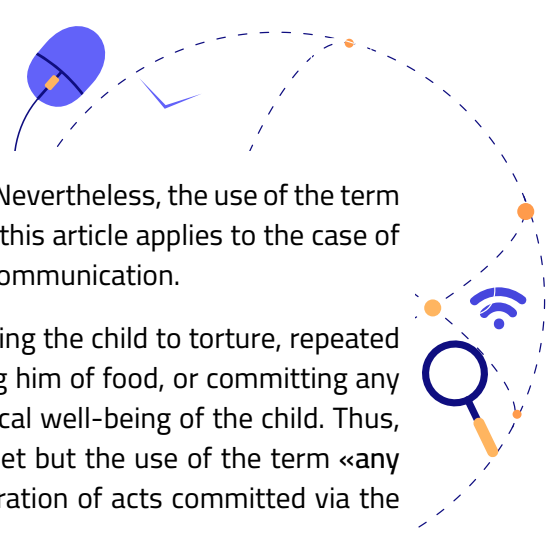
Article 2 provides that: 'For the purposes of this Law, the following means:

- Trafficking in persons: Trafficking in persons is considered to be the attraction, recruitment, transportation, transfer, diversion, repatriation, harbouring or receipt of persons, through the use or threat of use of force or weapons or any other form of coercion, abduction, fraud, deception, abuse of power or a vulnerable position or by offering or accepting money, benefits or gifts or promises of donations, in order to obtain the consent of a person having control over another person for the purpose of exploitation in whatever form, whether such exploitation is committed by the perpetrator or with a view to making that person available to a third party.
- Vulnerable situation: Any situation in which a person believes that he or she is obliged to submit to exploitation resulting from, inter alia, the fact that he or she is a child, his or her irregular situation, the woman's state of pregnancy, extreme necessity, a state of serious illness or dependence, or a mental or physical deficiency that prevents the person concerned from resisting the perpetrator. »

8. Child Protection Code

The Code provides for the prevention of exploitation of children, male or female sexually and habitual abuse in Article 20 (which specifies situations of threat).

Article 25 stipulates that the sexual exploitation of the child, whether boy or girl, includes exposing the child to acts of prostitution either directly or indirectly, whether for consideration or gratuitously.



Indeed, this article did not directly mention abuse via the Internet. Nevertheless, the use of the term «indirectly» means that the legislator has left the possibility that this article applies to the case of online abuse since it constitutes a virtual and indirect method of communication.


Article 24, which stipulates habitual ill-treatment, means subjecting the child to torture, repeated violations of physical integrity, detention, or the habit of depriving him of food, or committing any act of brutality that is likely to affect the emotional or psychological well-being of the child. Thus, another time the legislator did not mention abuse via the Internet but the use of the term «any act of brutality likely to...» has left the door open to the consideration of acts committed via the Internet as acts of abuse.

Articles 31 and 32 of the Code introduced the obligation to report to the national protection officer about cases which constitute a threat to children. This obligation also includes persons bound by professional secrecy.

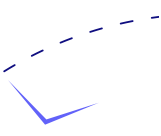
9. Law No. 2004-63 of July 27, 2004 on the Protection of Personal Data

Article 1 of Law No. 2004-63 of July 27, 2004 provides that «everyone has the right to the protection of personal data relating to their private life as one of the fundamental rights guaranteed by the Constitution and may only be treated within the framework of transparency, honesty and respect for human dignity, in accordance with the requirements of this Law. »

This Law is therefore applicable to all persons, adults or minors, and thus obviously applicable for children.



Article 28 required the consent of the guardian and the family judge with regard to the processing of personal data relating to children. The best interests of the child are the legal requirement for granting such permission.



Article 30 prohibits the processing of children's data for advertising purposes without the consent of the guardian and the family judge. The same procedure is required for the case of transfer of such data (Article 47).

Art. 90 of that Law states:

«Anyone who:

- intentionally carries out the processing of personal data without presenting the declaration provided for in Article 7 or without obtaining the consent provided for in Articles 15 and 69 of this Law, or continues to carry out the processing of data after the prohibition of processing or the withdrawal of the authorisation;
- disseminates personal data relating to health notwithstanding the prohibition of the Authority mentioned in the second paragraph of Article 65 of this Law;
- transfer of personal data abroad without the authorization of the Commission;
- communicates personal data without the consent of the person concerned or the consent of the Authority in the cases provided for by this Law.

In addition, Article 93 of the Law states that «anyone who intentionally disseminates personal data, in the course of their processing, in a manner that harms the data subject or his or her privacy shall be punished by three months' imprisonment and a fine of three thousand dinars.

The penalty is one month's imprisonment and a fine of one thousand dinars when the dissemination was carried out without the intention of harm.

The person concerned may request the court to order the publication of an extract from the judgment in one or more daily newspapers published in Tunisia chosen by the person concerned.

The costs of publication shall be borne by the convicted person.

Prosecutions can only be initiated at the request of the person concerned.

The withdrawal shall stop the prosecution, trial or execution of the sentence.»

10. Decree-Law No. 2022-54 of September 13, 2022, on the Fight against Crimes Relating to Information and Communication Systems

Article I specifies the scope of the text: «The purpose of this Decree-Law is to lay down the provisions aimed at the prevention of offences relating to information and communication systems and their punishment, as well as those relating to the collection of related electronic evidence and to support the international effort in this field, within the framework of international, regional and bilateral agreements ratified by the Republic of Tunisia. »

On the other hand, Article 3 insists that the offences mentioned in the decree-law are applicable to the provisions of the Criminal Code as well as other texts. Paragraph 2 provides that «children are subject to the Child Protection Code. »

Article 21 states that «anyone who deliberately misappropriates computer data belonging to others shall be punished by five years' imprisonment and a fine of thirty thousand dinars.

The attempt is punishable.»

Despite the general purpose of the text, he specified some cases of abuse against minors and this in Article 26 which states:

«Subject to specific legislation, anyone who intentionally produces, displays, provides, publishes, sends, obtains or possesses computer data with pornographic content showing or being a victim of a child or a person with the appearance of a child engaged in explicit or suggestive sexual practices shall be punished by imprisonment for six years and a fine of fifty thousand dinars.

Any person who intentionally uses information systems to publish or disseminate images or video footage of physical or sexual assaults on others is liable to the same penalties provided for in the first paragraph of this article.»

Thus, the Decree-Law criminalized the intentional possession/acquisition, production, publication and sending of pornographic content or content related to sexual practices concerning children.

This review of the legal framework reveals that, while there are various siloed texts that can be applied in crimes of cyberviolence against children, the lack of legal clarity means that the effectiveness of prosecutions depends on the jurisprudence.

II. The institutional framework for online child protection in Tunisia

This section provides an overview of the institutional actors involved in child protection. In particular, the procedures and institutions involved in child protection are the same as those involved in protecting and combating online violence against children.

1. Police and National Guard Services:

1.1. Specialized units to investigate crimes of violence against women

Article 24 of Organic Law No. 2017-58 of August 11, 2017, on the Elimination of Violence against Women:

«Established within each National Security and National Guard police station in all governorates a specialized unit to investigate offences of violence against women in accordance with the provisions of this Law. It must include women among its members. »

These brigades have since been created in accordance with this Law since February 2018. There are currently 70 brigades at the national security level, 58 at the national army level and two central brigades. Figure 1 below illustrates the structure of the regional units.

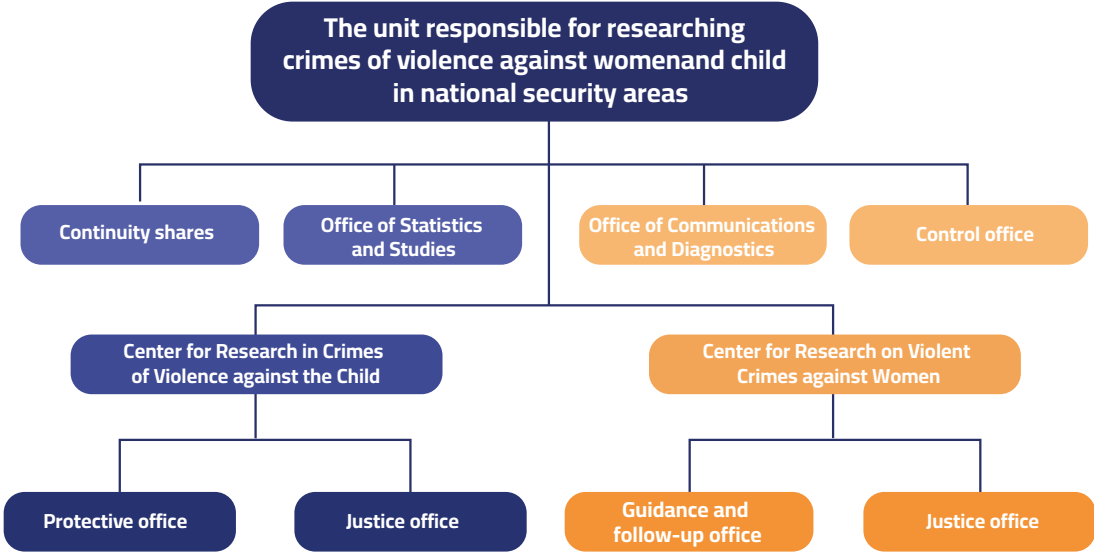


Figure 1: Structure of specialized units for investigating crimes of violence against women and children

The protection tasks of these units are defined in Article 26 of the same Law, which stipulates:

«The specialized unit may, with the authorization of the public prosecutor, and before the protection order is issued, take one of the following means of protection:

- the transfer of the victim and the children residing with him, if necessary, to secure places, in coordination with the competent structures and the child protection officer,
- the transfer of the victim to receive first aid when he suffers bodily injury,
- remove the accused from the home or prohibit him from approaching the victim or being in the vicinity of his home or place of work, in case of danger threatening the victim or his children residing with him.

Protection proceedings continue to take effect until the protection order is issued. »

1.2. The Juvenile Prevention Brigade

It is a central brigade created in 1966 and organized by Decree No. 2007-246 of August 15, 2007, establishing the structures of the internal security forces at the Ministry of the Interior and Local Development. It is responsible for investigations in relation to children at risk and children in conflict with the law.

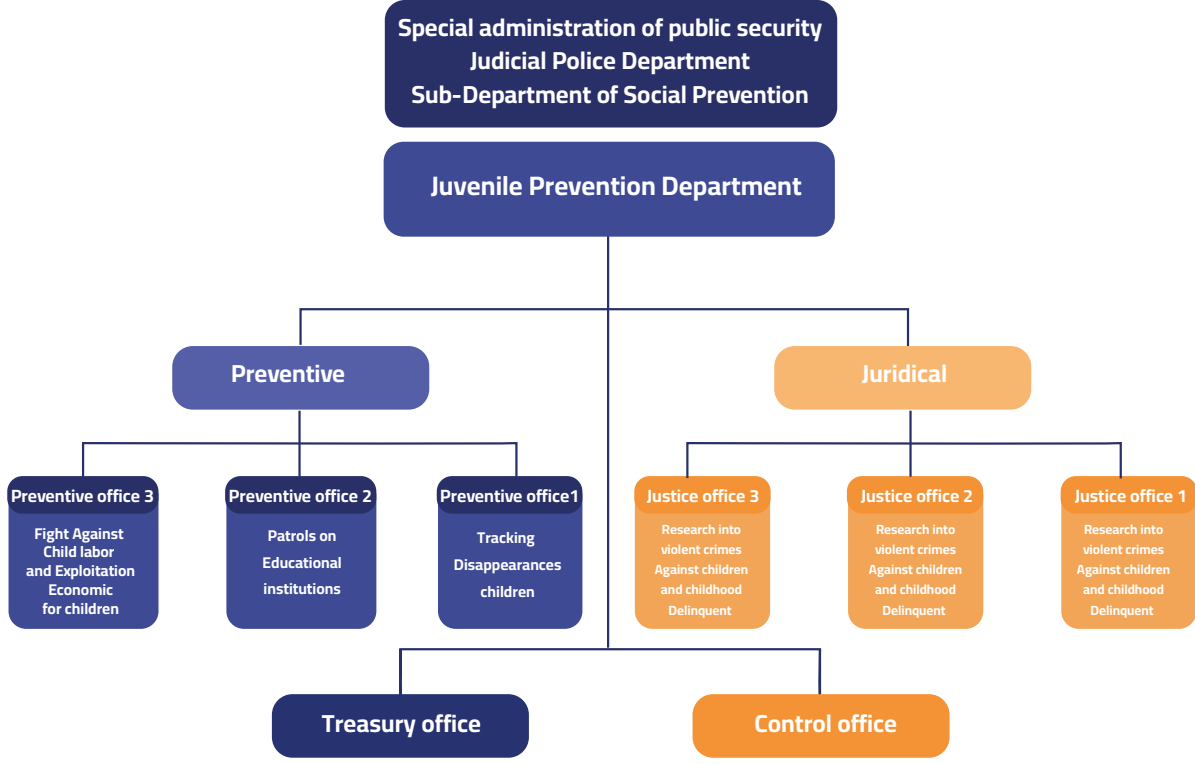


Figure 2: Structure of the Juvenile Prevention Brigade

1.3. Anti-Human Trafficking Brigade:

It was established in accordance with Organic Law No. 61 of 2016 of August 3, 2016 on Preventing and Combating Trafficking in Persons of offences related to trafficking in persons, including children.

1.4. The Social Welfare Sub-Directorate of the National Guard

It is committed to investigating crimes against children at the national level. This sub-directorate coordinates with specialized units such as the Technical Authority and the Technical and Scientific Police.

The competent units are required to investigate crimes of violence against children in coordination with the child protection officers throughout the country.

There are also units (research centres on crimes of violence against children in specialised units) in all areas of national jurisdiction.

1.5. The Technological Crime Brigade

It is located both in the General Directorate of National Security and in the General Directorate of the National Guard. This brigade deals with investigations into Internet crimes and communication crimes, both against children and adults, and works in constant contact with telecommunications operators, Internet service providers and the Tunisian Telecommunications Agency.

2. Child Protection Officer (CPO)

It is a preventive intervention structure in all difficult situations that threaten the health of the child or his physical or moral integrity, provided for in Article 20 of the Child Protection Code. The ECD is responsible for coordinating between the various actors concerned with children (social affairs, justice and human rights, public health, education and training, the Ministry of the Interior and local development...), as well as associations and organizations, and based on the principle of the best interests of the child.

The child protection officers report to the ministry responsible for children and act on a report.

Reporting is a protection mechanism based on informing the child protection officer if a situation of physical or moral threat is noticed on a child under 18 years of age. According to Article 31 of the Child Protection Code, reporting is a duty for all citizens, including those bound by professional secrecy such as doctors and lawyers.

Reporting is made by any means, by telephone, letter or electronically through the website of the child protection officers. The law prohibits the disclosure of the identity of the person who made a report and imposes penalties on those who reveal his identity.

3. Judicial authorities

3.1. The Family Judge

He or she is a second-grade judge specializing in threatened children located in the courts of first instance. According to Article 58 of the Child Protection Code (CPE):

- «The family judge shall hear the child, his or her parents or the person responsible for child custody, or guardian.
- He receives the observations of the representative of the Public Prosecutor's Office, the Child Protection Officer, and if necessary the lawyer.
- He may decide pleadings without the presence of the child, for his interest. »

According to Article 59 of the Code,

«The family judge may order one of the following measures:

- (1) to keep the child with his or her family;
- (2) keep the child with his or her family and instruct the child protection officer to monitor the child, help and guide the family;
- (3) subject the child to a medical or psychological check-up;
- (4) placing the child under guardianship or entrusting the child to a foster family or to a special social or educational institution;
- (5) place the child in a training centre or school. »

Article 51 of the CPE specifies the cases in which the family judge may be asked to take charge of the child at risk, on the basis of a simple request from the juvenile judge, the Public Prosecutor's Office, the child protection officer, public social welfare services and public institutions responsible for children's affairs. The family judge may take up the cases cited in the CPE himself or herself.

It should be noted that the family judge supervises the interventions of the child protection officer during the social protection phase.

3.2. The Public Prosecutor's Office

The Public Prosecutor's Office instructs the family judge for any difficult situation that puts a child in danger. As the judicial authority that monitors the various offences committed and receives complaints, notifications and reports transmitted by judicial police officers, the Public Prosecutor's Office is able to identify the difficult situations to which the child is exposed. In addition, it is the first instance likely to become aware of the situation of the child at risk in civil cases in which the child is a party or when the Public Prosecutor's Office has been involved in a case involving a minor, such as actions challenging filiation.

The Public Prosecutor's Office may also assign to the family judge any case in which a child under the age of 13 has committed an offence, but who is irrefutably presumed not to have the capacity to infringe the criminal law.

3.3. The juvenile investigating judge

Although Article 51 of the CPE did not provide for the possibility of referral to the family judge by the investigating judge for children, article 92 allowed the investigating judge to take a decision «of dismissal» and to refer the case to the family judge if he deems it necessary in situations where there is no evidence that the child has committed an offence punishable by law, but where the child seems threatened.

The matter may be referred to the family judge on the basis of a written or verbal report from the investigating judge for children or the investigating judge, the purpose of which is to report a case of threat if the latter has noted this situation during the performance of his duties (following the hearing of a child victim or witness).

4. The National Authority for the Protection of Personal Data (INPDP)

This body began exercising its prerogatives in 2009, following the appointment of its members in 2008. Its creation is enshrined in Organic Law No. 2004-63 on the protection of personal data, adopted on July 27, 2004, while its operation was subsequently determined by Decree No. 2007-3003 of November 27, 2007. Its mission is to ensure compliance with the provisions of the Data Protection Act by implementing the means necessary for the exercise of its mandate, such as procedural manuals, training and awareness campaigns.

Article 76 of Organic Law No. 2004-63 stipulates:

«The National Authority for the Protection of Personal Data is responsible for

Following missions :

- grant authorizations, receive declarations for the implementation of the processing of personal data, or withdraw them in the cases provided for by this law ;
- receive complaints made within the scope of the jurisdiction assigned to it under this Law ;
- determine the necessary safeguards and appropriate measures for the protection of personal data ;
- access the personal data being processed in order to verify them, and collect the information essential for the performance of its tasks ;
- give its opinion on any subject related to the provisions of this law ;
- develop rules of conduct for the processing of personal data ;

- participate in research, training and study activities related to the protection of personal data, and in general in any activity related to its field of intervention».

Article 77 of the same Law authorizes the body to

carry out the necessary investigations by taking statements from any person whose hearing is considered useful and by ordering findings to be made in the premises and places where the treatment took place, with the exception of residential premises. The Commission may be assisted, as part of its missions, by the sworn agents of the Ministry in charge of communication technologies to carry out specific research and expertise, or by judicial experts, or by any person deeming its participation useful.

The Commission must inform the territorially competent public prosecutor of all offences of which it has become aware in the course of its work.

Professional secrecy may not be invoked against the proceedings. »

5. National Body for Combating Trafficking in Persons (IN-LTP)²

This body was created under Organic Law No. 2016-61 of August 3, 2016 on the Prevention and Fight against Trafficking in Persons. The commission's missions include the development of a national strategy to prevent and combat trafficking, as well as the establishment of coordinated mechanisms for identifying, caring for and protecting victims, reducing demand and prosecuting perpetrators. Thus, the first national strategy to combat trafficking in persons in Tunisia was launched in July 2018 for the period 2018-2023.



6. Coordination with educational institutions

Coordination is very important with this stakeholder, not least because of its particularities at all levels.

The judge must be attentive to sensitivities that may affect the coordination process, especially if the judge's decisions conflict with the orientations of the educational institution. In order to avoid these problems, the judge may, before making any decision affecting the child's educational status, communicate directly or through the child protection officer with the regional education delegations, or request reports and proposals. Representatives of the administration may also be summoned for a hearing.

In addition to coordination with the administration, the judge may also coordinate directly or administratively with the psychologist belonging to the service of the regional education delegations, and the latter may attend the hearings, but his summons requires compliance with administrative procedures.

² <https://www.coe.int/en/web/portal/-/tunisia-launches-new-initiative-to-better-detect-and-help-victims-of-human-trafficking>

7. IWF Tunisia Photo and Video Reporting Portal

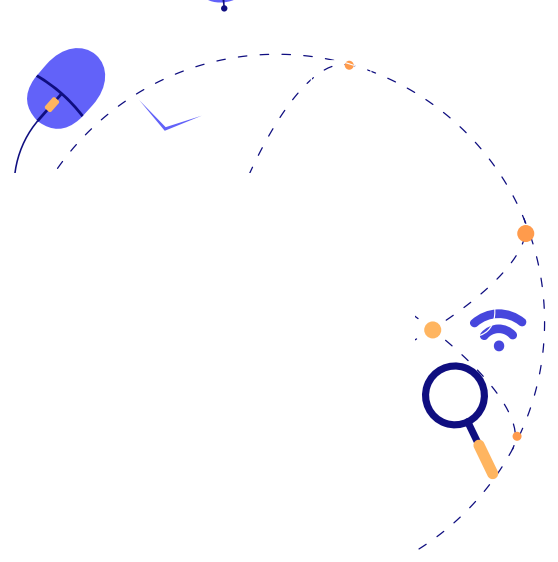
The portal to protect children from online abuse and exploitation was launched on June 10, 2021, by the Ministry of Women, Family and Seniors of Tunisia and Internet Watch Foundation (IWF), in cooperation with the Global Partnership 'End Violence against Children, the Council of Europe in the framework of the joint programme with the European Union (South Programme IV1)), and the United Nations Children's Fund (UNICEF).

Tunisia thus becomes the 47th country in the world with a portal of this type set up by IWF, the 23rd in Africa and among the very first in North Africa and the MENA region.

The spread of child sexual abuse materials on the Internet is a global phenomenon requiring both national ownership and enhanced international cooperation.

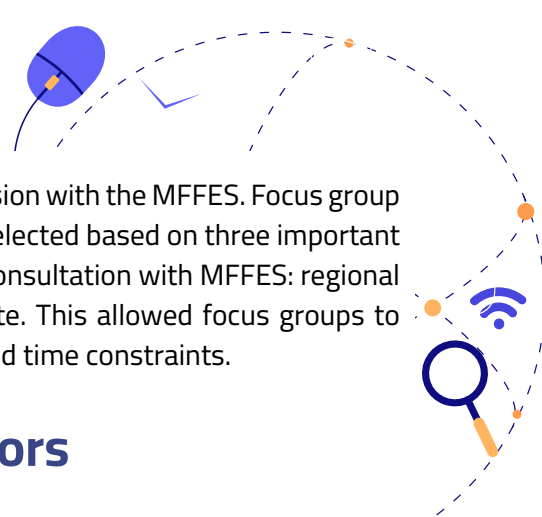
This reporting portal contributes to the national process of prevention and protection against sexual violence against children and to the empowerment of society. It will allow Tunisian citizens to securely and anonymously report images and videos of child sexual abuse posted on the Internet with a view to removing them.

Link to the reporting portal in Tunisia: <https://report.iwf.org.uk/tn>



Annex 3: Indicators for the selection of research sites






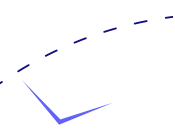
The research sites were determined after consultation and discussion with the MFFES. Focus group locations in Gafsa, Kasserine, Jendouba and Greater Tunis were selected based on three important and interconnected indicators of child vulnerability developed in consultation with MFFES: regional development indicators, baccalaureate pass rate and dropout rate. This allowed focus groups to respond to research needs while taking into account budgetary and time constraints.

I. The regional development indicators


Regional disparities, due to decades of uneven development policies in Tunisia, have led to increased vulnerabilities faced by children in inland rural areas compared to their peers in coastal urban areas. Indeed, there are conceivable differences in knowledge, use and awareness of ICTs and the risks associated with them, as well as in reporting between children living in rural and urban areas. It can also be a factor in both the use of different applications, risk exposure, and the relationship between online and offline risks. To quantify this disparity, this research uses the Regional Development Index developed by the Tunisian Institute of Competitiveness and Quantitative Studies (ITEQ). The index reveals disparities in development between coastal regions and the interior of countries, with the governorates of Kasserine, Kairouan and Jendouba consistently ranking lowest between 2015 and 2018. The¹ 2021 index also reveals that «the interior regions (Kasserine, Kairouan, Jendouba, Sidi Bouzid) occupy the last ranks in the regional development grid, they constitute the most disadvantaged areas compared to the rest of the country.»²



In Tunisia, historical regional socio-economic inequalities have been compounded by a «digital divide» that disadvantages marginalized children in poor interior regions. Children represent 29% of the Tunisian population, and they represent 40% of the country's poor. In addition, children living in rural interior areas are at increased risk of living in poverty or extreme poverty. This precariousness has been further exacerbated by Covid-19, with poverty rates raising from 15.2% to 19.1% and extreme poverty from 2.9% to 3.3%. The pandemic has highlighted existing inequalities in access to technology and broadband, especially outside urban centres. This impacts both access to technology and technology infrastructure, but also the digital literacy of children and youth online.³



Unequal access to adequate educational infrastructure and services, due to these regional inequalities, has led to higher drop-out rates in primary and secondary schools and higher baccalaureate failure rates in the interior regions.



¹ Boussida, S et al. (2019) The Regional Development Index 2021. The Tunisian Institute of Competitiveness and Quantitative Studies (ITEQ) <http://www.itceq.tn/files/developpement-regional/indicateur-de-developpement-regional-2019.pdf>

² Boussida, S et al. (2022) Regional Development Index 2021. The Tunisian Institute of Competitiveness and Quantitative Studies (ITEQ) <http://www.itceq.tn/files/developpement-regional/indice-dev-regional-2021.pdf>

³ Ministry of Women, Family, Childhood and Seniors (2021) Integrated Public Policy for the Prevention and Protection of Children Project. p. 4 <http://www.femmes.gov.tn/wp-content/uploads/2017/07/Resum%C3%A9- Unequal access to adequate educational infrastructure and services, due to these regional inequalities, has led to higher drop-out rates in primary and secondary schools and higher baccalaureate failure rates in the interior regions.executive.pdf>

II. To the success of the baccalaureate

Failure in the most important national examination of the Tunisian education system is a key indicator of social and economic marginalization. In 2021, the wealthiest coastal regions of Sousse and Monastir recorded baccalaureate pass rates of 61% and 62.5% respectively, while Jendouba (35.7%), in the Northwest, followed by Gafsa (37.39%), in the south, had the lowest Baccalaureate pass rates.⁴

III. School drop-out rate

Research on the likelihood of dropping out of school shows a significant association with negative life events – including, among others, the child’s physical and mental problems and parenting problems^{5,6}

In addition, research shows a clear interconnection between regional (under)development on the one hand and early school leaving on the other. Indeed, «school failure mainly affects the North-West regions, so half of the school population, in governorates such as Jendouba and Beja, drops out of school.

There are several factors responsible for this failure: remote school, obligation to stay at home, very expensive school supplies... Kasserine has the highest drop-out rate (2.3%) in Tunisia.⁷⁸

These three indicators are closely related and should be understood as such. Regional inequalities in turn generate and exacerbate other vulnerabilities that can directly put children at greater risk of various types of violence. Children with lower levels of digital literacy may be disadvantaged when education is online, resulting in lower academic outcomes than their peers (assuming they can even connect), itself a risk factor for violence. These children may also be more vulnerable to certain types of violence that occur both online and offline, such as radicalization and sexual exploitation of children online.

4 Bac.org.tn (2021) Bac Tunisia 2021: Success rates by section and region. <https://bac.org.tn/bac-tunisie-2021-taux-de-reussite-par-section-et-par-region/>

5 Gubbels, J., van der Put, C.E. & Assink, M. Risk Factors for School Absenteeism and Dropout: A Meta-Analytic Review. *J Youth Adolescence* 48, 1637–1667 (2019). <https://doi.org/10.1007/s10964-019-01072-5>

6 Samuel, R., & Burger, K. (2020). Negative life events, self-efficacy, and social support: Risk and protective factors for school dropout intentions and dropout. *Journal of Educational Psychology*, 112(5), 973–986. <https://doi.org/10.1037/edu0000406>

7 Daghari, S., and Ben Rabah, I., (2022) State of play and disparities of the Tunisian education system. *Tunisian Institute of Competitiveness and Quantitative Studies (ITEQ)* p.6.

8 Daghari, S., and Ben Rabah, I., (2022) State of play and disparities of the Tunisian education system. *Tunisian Institute of Competitiveness and Quantitative Studies (ITEQ)* p.11



HOTLINE NUMBER

ASSISTANCE, GUIDANCE AND REPORTING