TOWARD SAFE DIGITAL SPACES:
THE IMPORTANCE OF LEGISLATION TO ADDRESS ONLINE VIOLENCE IN IRAQ AND THE KURDISTAN REGION

Image: A young woman attends one of SEED's awareness sessions on online safety. Duhok, Iraq. ©SEED, 2024

Toward Safe Digital Spaces:
The Importance of Legislation to Address Online Violence in Iraq and the Kurdistan Region

Author: Kristin Perry, Senior Policy and Advocacy Advisor at SEED

Acknowledgements: The author would like to extend her gratitude to Adnan Qadir for his invaluable contributions, and to all reviewers for their feedback and revisions.

Date of Publication: June 2025

SEED is a women-led, local NGO in the Kurdistan Region of Iraq, dedicated to creating a thriving society by advancing social protection and human development. We support individuals, empower communities, and strengthen systems to drive lasting change and access to equal opportunity. With a focus on collaboration, we promote gender equality, protect children, combat human trafficking, and improve mental health and well-being. Our holistic, locally-driven approach integrates transformational services, community development, training and education, and advocacy to create sustainable impact. SEED is committed to creating a just, equitable society where everyone's rights are protected, with healthy families and strong communities, and a future where everyone can thrive.

This publication has been produced with financial support from Safe Online. However, the opinions, findings, conclusions, and recommendations expressed herein are those of the author and do not necessarily reflect those of Safe Online.

Table of Contents

Introduction

Online violence has emerged as a new and insidious threat in Iraq and the Kurdistan Region, with profound implications for the well-being of all, but particularly grave consequences for already vulnerable groups, including women and children. Considerable work is being done to combat online violence within the confines of the current legal framework, but critical gaps and deficits remain. Strong legislation is needed to regulate online behaviors and support a holistic, comprehensive response to violations in the digital dimension. Crafting legislation on this topic is a complex and delicate process, however. Legislators must balance protected interests to prevent harm while preserving fundamental rights and freedoms, and must achieve clarity and precision while maintaining the flexibility to address new forms of criminal activity in a dynamic and rapidly evolving landscape. Despite these challenges, legislation provides an essential foundation that shapes all aspects of response, and is therefore considered a key strategy in the fight against online violence.[1]

Understanding Online Violence

Online violence[2] refers to a broad array of harmful acts or behaviors that may be threatened, committed, facilitated, or aggravated through the use of information and communications technology (ICT). It is a distinct category of violence, perpetrated via technological means, that requires specialized strategies to address. The impact of online violence is not confined to the virtual world, however. These violations are real and dangerous, capable of causing significant physical, psychological, social, and economic harm to victims and survivors. Additionally, such acts often intersect with, arise from, or result in offline violations as part of a continuum of violence, functioning as a threat multiplier.

Online violence reinforces and replicates patterns of violence that exist outside of the digital dimension. As in the physical world, those at highest risk are often members of vulnerable groups, including women and children. Women are disproportionately affected by technology-facilitated gender-based violence (TFGBV), an umbrella term encompassing diverse violations against women that are enabled or amplified through technology. Common examples in Iraq and the Kurdistan Region include online harassment, bullying, and image-based sexual abuse (IBSA) – a serious violation which may involve creating, taking, or sharing intimate images or videos without consent, or threatening to do so for coercion, defamation, exploitation, blackmail, or other harmful purposes.[3] Children, meanwhile, are at grave risk of technology-facilitated child sexual exploitation and abuse (TF-CSEA)[4], which refers to a spectrum of sexual offenses against children that involve the use of digital technologies, including subjection to sexual acts; coercion to perform sexual acts; access to, production, distribution, or possession of child sexual abuse materials (CSAM) or child sexual exploitation materials (CSEM); and the solicitation and grooming of children for such purposes. As of 2023, Iraq ranked 10th highest in the world for reported cases of TF-CSEA, both in terms of the overall number of reports and the percentage of reports relative to its population.[5] [6]

1 For further information and a detailed examination of the themes in this paper, please see SEED's forthcoming publication, *Legislative Analysis: Online Violence in Iraq and the Kurdistan Region (2025).*

2 The term "online violence" is used in this paper to connect to the dominant discourse in Iraq and the Kurdistan Region. This term is often used interchangeably with "technology-facilitated violence," and should not be understood to exclude the role of ICT and digital technologies in enabling or amplifying harms more broadly, in both digital and non-digital environments, from consideration.

3 Violence Against Women in the Online Space (UN Women, 2021); National Survey (SEED, 2023).

4 The term "online child sexual exploitation and abuse," or OCSEA, is also common in the existing discourse. However, the use of "technology-facilitated" as a central qualifier, rather than "online," increases definitional accuracy and breadth, better reflecting the role of technology in enabling or amplifying these crimes against children. For more information, see the second edition of Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT International, 2025), Section G.

5 2023 CyberTipline Reports By Country (NCMEC, 2023).

6 TFGBV and TF-CSEA are referenced throughout this paper, not because they comprise an exhaustive set of potential violations against women and children, but because they are emblematic of those violations.

Online violence is a relatively new and continuously evolving threat, which has increased in both prevalence and severity as a greater proportion of social interaction moves into the virtual sphere. Its rise has been facilitated by rapid digitalization, the proliferation of digital technologies, and heightened usage patterns, with the number of internet users in Iraq projected to reach 98% this year,[7] and has been exacerbated by gaps in digital literacy that impact the ability of at-risk populations to protect themselves, practice safe online behaviors, and successfully navigate technology-mediated environments. In many countries around the world, technological advancements and associated risks continue to outpace policy responses, leaving governments struggling to identify agile, adaptive solutions to address online violence. While this is a global challenge, the implications in Iraq and the Kurdistan Region – where rates of violence against women and children are already high, protection mechanisms are inadequate, and sociocultural dynamics introduce compounding risks of honor-based stigma and reprisals for survivors – are especially profound.

The Role of Legislation in Addressing Online Violence

Crime is dynamic. As it evolves, legal frameworks and systems must adapt in response. While it is possible to address certain forms of online violence within applicable criminal laws that govern the management of traditional offenses, these legislative tools were not designed for use in the digital age. As such, they may not be sufficient to respond to rapid technological advancements, recognize emerging forms of criminal behavior, or establish appropriate protocols for the investigation and prosecution of those acts, including through the preservation and management of electronic evidence.[8] For this reason, the enactment of clear and comprehensive legislation is considered a key strategy in the fight against online violence.

Legislation provides a critical foundation for an effective response to online violence. By criminalizing specific offenses and delineating penalties, as well as integrating measures for prevention, protection, prosecution, and reparation, legislation establishes expectations and standards for appropriate conduct online and provides a framework for public accountability when those standards are violated. In this way, the enactment of a law not only serves to preserve rights and provide safety in the digital sphere, but also ensures that online crimes can be recognized, reported, investigated, and prosecuted as such, and that victims can access justice, recourse, and support in the aftermath of harm. Without it, the response to online violence can be ad hoc, inconsistent, or limited, creating vulnerabilities that can be exploited by both domestic perpetrators and foreign cybercriminals looking to operate in countries with weak or nonexistent legal frameworks. [9]

Crafting legislation on this topic is admittedly difficult, however, requiring lawmakers to navigate considerable complexity in order to avoid common pitfalls and ensure the quality and efficacy of the resulting framework. Laws that seek to regulate behaviors in the digital environment may be vulnerable to misapplication and abuse, particularly in the context of authoritarian regimes or surveillance states. Legislators must therefore strike a delicate balance between protected interests to prevent harm and combat crime while preserving fundamental rights and freedoms.[10] This may require the integration of both substantive and procedural safeguards, guided by core human rights standards and the principles of legality, necessity, proportionality, and non-discrimination. Additionally, given the explosive pace of technological advancement, laws enacted to address existing forms of online violence risk becoming irrelevant or obsolete within a short term time horizon. Considerable foresight is required to legislate with clarity and precision while maintaining sufficient breadth and flexibility to allow for adaptation and application to emerging forms of criminal activity.[11]

It is also important to recognize that legislation alone, while essential, is not enough. In order to deter potential

7 As per Statista's Digital & Connectivity Indicators for Iraq.

8 A systematic literature review on cybercrime legislation (Khan, Saleh, Dorasamy et al., 2022).

9 What is Cybercrime and how can you prevent it? (Brush and Cobb, 2024).

10 Global perspectives on cybercrime legislation (AllahRakha, 2024, p. 9).

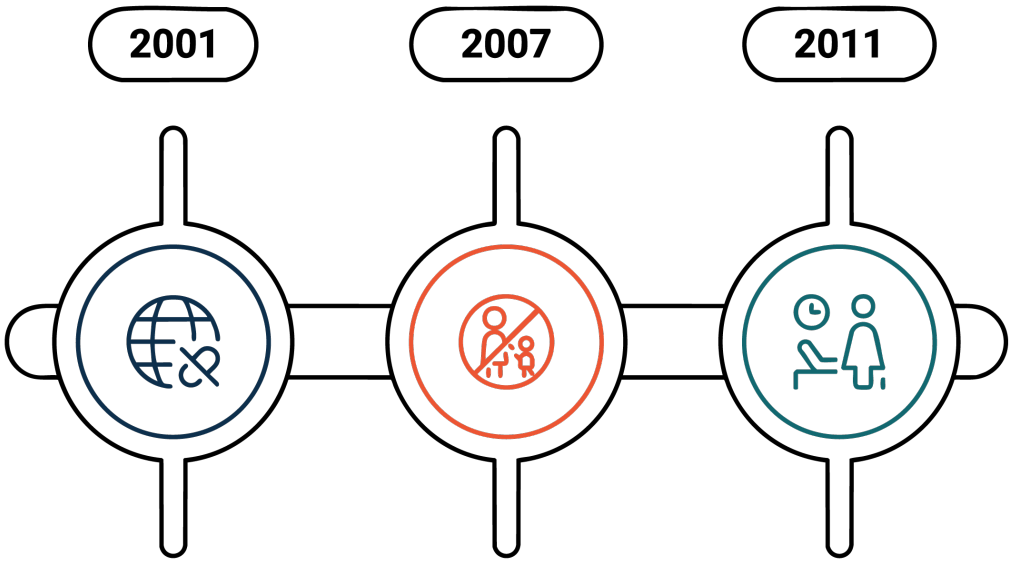
11 Ibid, pp. 15 ,10-9.

perpetrators of online violence and encourage victims to report violations and seek assistance, laws must be enacted in an environment of accountability, rather than impunity, and must be complemented by consistent and impartial enforcement. Given the complex nature of these crimes, adequate institutional capacity, technological infrastructure, technical expertise, and resources are also required to support effective implementation. Furthermore, the legislative framework itself, while of paramount importance, must be understood as one core component of the overall solution. Online violence is a complex, multifaceted phenomenon that requires holistic and multidimensional interventions. A "whole systems" approach to combating online violence – with integrated, coordinated policies and multi-stakeholder, cross-sectoral collaboration and action – is needed to ensure the efficacy of prevention, mitigation, and response strategies.

Relevant International Standards

Since the turn of the century, as the world gradually shifted from its reliance on analog to digital technologies, a number of international conventions have been enacted that provide benchmarks for the protection of human rights in the digital dimension, including three landmark frameworks produced by the Council of Europe (COE).

Key Council of Europe Conventions



The *Convention on Cybercrime*, or Budapest Convention, adopted in 2001, was the first binding international treaty to address online violations. It provides guidelines for the issuance of comprehensive, domestic criminal laws – integrating both substantive and procedural measures – to promote a common framework for combating cybercrime and to foster international cooperation in addressing this transnational threat. The Budapest Convention criminalizes a variety of offenses perpetrated via the internet and other computer networks, ranging from illegal access, data, and systems interference to computer-related fraud and child pornography.[12] The Cybercrime Convention Committee (T-CY) Working

12 The term "child pornography" is used in the text of the Budapest and Lanzarote Conventions. However, the terms "child sexual abuse material," or CSAM, and "child sexual exploitation material," or CSEM, are increasingly being used to replace the term "child pornography," as they are less stigmatizing and encompass a broader set of materials. For more information, please see the second edition of Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT International, 2025), Section F.4.i.

Group on Cyberbullying and Other Forms of Online Violence Especially against Women and Children subsequently harmonized the provisions of this convention with other frameworks on the protection of women and children, such as the Istanbul and Lanzarote Conventions, and established its relevance to acts of online violence or acts facilitating online violence,[13] which it defines as "the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities."[14] This definition covers a range of offenses, including cyberbullying, cyberharassment, defamation, coercion, threats of violence, blackmail, extortion, sextortion, IBSA, stalking, doxxing, and TF-CSEA, among others.

In 2007, the adoption of the *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, or Lanzarote Convention, expanded available guidance on the implementation of legislative measures to protect children. This convention represents the first regional treaty specifically dedicated to protecting children from sexual violence, as well as the first international legal instrument that criminalizes the act of grooming. In addition to criminalizing various forms of child sexual exploitation and abuse – including prostitution,[15] pornography, participation of a child in pornographic performances, corruption of children, and solicitation of children for sexual purposes – and establishing procedures for the investigation and prosecution of these offenses, the Lanzarote Convention also outlines preventative measures for the screening, recruitment, and training of those in contact with children, as well as awareness for children themselves; monitoring measures for offenders and potential offenders; reporting mechanisms and helplines to facilitate intervention; and programs to provide victim support and assistance. The Lanzarote Committee subsequently issued an Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offenses against children facilitated through the use of information and communication technologies (ICTs), as well as a Declaration on protecting children against sexual exploitation and sexual abuse facilitated by emerging technologies, which establish the applicability of the convention to online violations and call upon State Parties to protect children against sexual exploitation and sexual abuse facilitated via these means.

In 2011, the Council of Europe adopted the *Convention on Preventing and Combating Violence against Women and Domestic Violence*, or the Istanbul Convention. This innovative framework recognizes violence against women as a violation of human rights and a form of discrimination, and is the first legally binding instrument in Europe to establish specific standards for prevention, protection of victims, provision of support services for survivors and those at risk, and prosecution of perpetrators. Within this comprehensive and holistic approach, the Istanbul Convention obligates State Parties to criminalize various forms of violence against women, including by introducing new offenses; ensure effective investigation and victim-centered judicial proceedings; provide appropriate and accessible protection and support services, such as shelters, crisis centers, and helplines; and invest in awareness campaigns, education, and training for professionals in contact with victims, as well as treatment programs for perpetrators. Notably, the convention also recognizes the importance of sustained commitment and collective action from diverse stakeholders at every level, and calls for the development of integrated, coordinated policies to support a "whole systems" approach to eradicating violence. The convention's Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) subsequently adopted its first General Recommendation on the Digital Dimension of Violence Against Women, dedicated to establishing the applicability of the Istanbul Convention to violations perpetrated in the digital sphere and/or facilitated by technology, including numerous offenses that fall within the broad categories of online sexual harassment, online and technology-facilitated stalking, and psychological violence.

While Iraq has not acceded to these frameworks, the Council of Europe standards contained in the Budapest, Lanzarote, and Istanbul Conventions, along with their associated soft law provisions, "offer valuable benchmarks, guidance, and

13 Referred to as "cyberviolence" by the T-CY, although the two terms are used interchangeably.

14 Mapping Study on Cyberviolence (COE T-CY, 2018, pp. 6-5).

15 The term "prostitution" is used in the text of the Lanzarote Convention. However, the term "exploitation of children in/for prostitution" is a preferable alternative, as it is less stigmatizing and clearly establishes that children used in this way are victims of exploitation. For more information, please see the second edition of Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT International, 2025), Section E.

tools to states in tackling violence in the digital environment,"[16] and can be used to inform the development of robust, comprehensive domestic legislation to address online violence against women and children.

More recently, in December 2024, following five years of multilateral negotiations, the United Nations (UN) General Assembly adopted the *UN Convention Against Cybercrime*, which represents the first international criminal treaty to have been enacted in more than 20 years, as well as the first binding UN instrument on a cyber issue, and has been recognized as a "significant milestone in the fight against cyber threats."[17] In contrast to the Budapest Convention, which has long served as the primary international framework for addressing cybercrime, the new UN Convention was negotiated by a more extensive and diverse set of member states. It has a broader mandate than the Budapest Convention, extending beyond a focus on criminalization, procedural powers, and evidence-sharing to address a wider range of issues, such as measures for the prevention of cybercrime and the protection of state sovereignty.[18] It also provides a more comprehensive framework for international cooperation that includes technical assistance and capacity-building for developing countries.[19] Notably, the convention explicitly criminalizes offenses related to online child sexual abuse or child sexual exploitation material, solicitation or grooming for the purpose of committing a sexual offense against a child, and the non-consensual dissemination of intimate images, providing a strong foundation for addressing TF-CSEA and prevalent forms of TFGBV in domestic legislation.[20] However, even this contemporary framework, considered to be a victory for multilateralism, has been criticized by human rights defenders, cybersecurity experts, and other stakeholders due to its insufficient safeguards and potential for misuse – underscoring the crucial need for balance in digital governance, as well as adherence to the principles enshrined in the Universal Declaration of Human Rights (UDHR) when translating these obligations into national law. While ratification of the UN Convention Against Cybercrime by 40 signatories is required for the agreement to enter into force, the adoption of this new treaty demonstrates increased global interest in, and prioritization of, the fight against cybercrime, as well as broad recognition of the need for legislative frameworks to address online threats.

The Legislative Environment in Iraq and the Kurdistan Region

Currently, the primary international instrument with direct applicability to the issuance of domestic legislation on online violence in Iraq and the Kurdistan Region is the *Arab Convention on Combating Information Technology Offenses*, adopted by the Arab States in 2010 and ratified by Iraq in 2013. Like its predecessor, the Budapest Convention, this treaty includes substantive provisions to criminalize information technology offenses, most of which are either forms of online violence in their own right or acts that facilitate online violence; procedural rules for the investigation of these offenses; and mechanisms for enhanced legal and judicial cooperation between state parties, with the ultimate aim of protecting the security and interests of the Arab States and the safety of their communities and individuals. In contrast to the Budapest Convention, however, this agreement has a stronger focus on maintaining the security of the State, fewer safeguards for the preservation of individual rights and civil liberties in the process of combating information technology offenses, and has not been as effectively harmonized with other relevant instruments for the protection of women and children in the digital dimension. As a State Party to the *Arab Convention on Combating Information Technology Offenses*, Iraq is obligated to integrate the provisions of this agreement within its domestic legislation. Despite these commitments, however, Iraq and the Kurdistan Region continue to lack clear, comprehensive, and coherent legal frameworks for addressing online violence.

16 Comments submitted by the Children's Rights Division of the Council of Europe on the UN Committee on the Rights of the Child concept note for a General Comment on children's rights in relation to the digital environment (COE, 2019, p. 3).

17 INTERPOL welcomes adoption of UN convention against cybercrime (INTERPOL, 2024).

18 Comparative analysis: the Budapest Convention vs the UN Convention Against Cybercrime (DigWatch, 2024).

19 Ibid.

20 See the United Nations Convention Against Cybercrime, Articles 16- 14.

In 2008, the Kurdistan Regional Government (KRG) passed a Law on Preventing Misuse of Telecommunication Devices, which is the most relevant piece of legislation enacted to date in the fight against online violence. Although the law does criminalize certain forms of online violence and delineate punishments for perpetrators, it does not comprehensively identify or clearly define all relevant offenses, nor directly address TFGBV or TF-CSEA – leaving some common violations to be addressed via other frameworks. Additionally, the law does not mandate a specialized government institution or agency to respond to online violence, nor introduce any special or technical procedures for the management of these offenses, relying instead on authorities and processes designed for offline violations. While the law does include basic accountability measures for telecommunication companies, such as a requirement to register all devices and SIM cards in the names of users and cancel those that remain unregistered, these provisions have yet to be implemented or enforced. Finally, the law lacks measures designed to prevent online violence, provide needed support to victims and survivors, integrate survivor-centered and rights-based approaches to criminal proceedings, or offer sufficient safeguards against the suppression of fundamental rights and liberties in the digital dimension.

In 2011, a draft Law on Combating Cybercrimes was introduced to the Iraqi Council of Representatives (COR), and was subsequently reintroduced in 2019. While there have been numerous attempts to legislate this draft since its creation, prevalent concerns about its shortfalls and potential to restrict freedom of expression have prevented passage.

In the absence of a comprehensive legal framework on this issue, some online violations may be addressed within the confines of laws designed to regulate traditional offenses, outside of the virtual dimension. These include the Iraqi Constitution of 2005, which prohibits all forms of violence and abuse in the family, school, and society;[21] the Iraqi Penal Code No. 111 of 1969, the primary law applicable to criminal behaviors, which prohibits acts such as threat, defamation, insult, disclosure of private information, sexual exploitation and abuse of children, and the creation, possession, or transportation of indecent materials, as well as the misuse of cable and wireless communication equipment to cause alarm;[22] and a number of specialized laws[23] on trafficking, prostitution, and domestic violence, which include provisions that may be interpreted to address online violations falling within the scope of the listed offenses or cases in which digital means are used in the process of committing such acts. In theory, while many forms of online violence may be covered within the "offline" provisions of existing domestic laws,[24] and may be investigated and prosecuted on that basis, differences in the subject matter relevance, scope of application, and institutions mandated to respond across these frameworks can blur lines of accountability and leave individual cases subject to variable interpretation and inconsistent adjudication. Some of these frameworks may even be used to prosecute victims of online violence, depending on the nature of the crime. Additionally, exponential advancements in digital technologies continue to create new means of criminal activity and ever-evolving uses of those means, introducing further complexities and considerations in the regulation of online conduct, and requiring modernized and adaptive methods of prevention, detection, and corrective action.

This amalgam of general and specialized laws, with varying degrees of applicability, creates substantial challenges in addressing online violence in Iraq. The current legislative environment leaves critical gaps that can be exploited by potential perpetrators,[25] contributing to high rates of violence against women and children. It also complicates the ability of relevant institutions to leverage an effective, consistent, and coordinated response, impeding equitable access to justice and support for those affected.

21 See the Constitution of the Republic of Iraq (2005), Article 4/29.

22 See the Iraqi Penal Code No. 111 of 1969, Articles 438-430 ,403-393 ,363.

23 For example, the Law of Combating Human Trafficking No. 28 of 2012 in Iraq and No 6. of 2018 in the KRI; the Law of Combating Prostitution and Homosexuality No. 8 of 1988 in Iraq and the Law of Combating Prostitution No. 8 of 1988 in the KRI; and the Law of Combating Domestic Violence No. 8 of 2011 in the KRI.

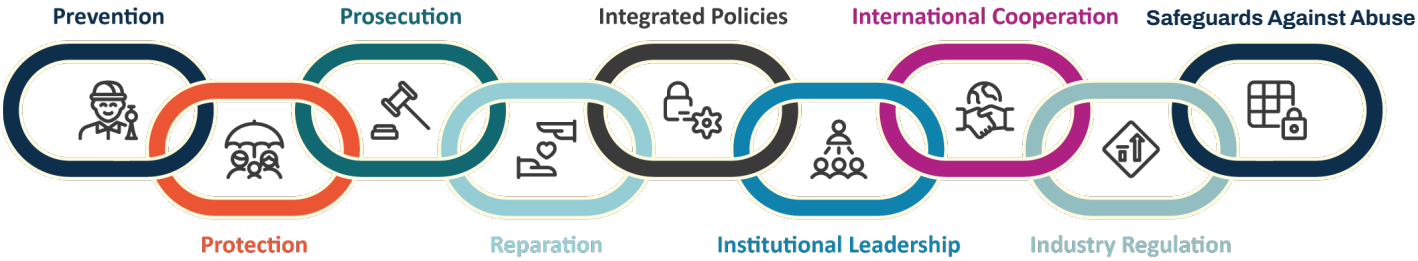
24 Mapping Study on Cyberviolence (COE T-CY, 2018, p. 5).

25 Cybercrime Laws in Iraq: Addressing Limitations for Effective Governance (Suleiman et al., 2023, p. 40).

What Constitutes a Strong Legislative Framework for Addressing Online Violence

Legislation to address online violence must be comprehensive and holistic, providing an actionable roadmap that can support the delivery of targeted interventions at every stage of response. It should therefore include provisions designed to prevent violence, protect victims, prosecute perpetrators, and provide reparation to those affected, as well as set a precedent for the development and implementation of coordinated policies – in all sectors and at every level – to build a whole systems approach to combating this significant threat. Due to the rapidly evolving digital landscape, legislation may also benefit from the integration of a monitoring mechanism, such as the establishment of a review process or committee, to periodically assess the efficacy of the framework and determine whether dynamic adaptations are needed to integrate emerging forms of online violence or establish applicability to them.

Core Components of a Strong Legislative Framework to Address Online Violence



As a first principle, legislation to address online violence should be developed through a robust participatory and consultative process, including with survivors, to ensure that their experiences, perspectives, and needs are recognized and reflected, and that the proposed solutions are responsive and appropriately contextualized. Rights-based, survivor-centered, and child-friendly approaches must be integrated throughout to ensure that survivors' dignity, well-being, and wishes form the basis for any action and remain at the center of all processes. This includes strong safeguarding, informed consent, and confidentiality protocols, recognizing that preserving the safety and security of survivors is of paramount importance, and understanding that response mechanisms can be misused and that new risks can be introduced by gathering additional data on sensitive violations or by taking action against a perpetrator.

Criminalizing online acts and behaviors is a process that must be approached with caution, as it has the potential to compromise certain applicable rights and freedoms in the digital dimension, including the rights to privacy and protection of personal data, as well as the freedoms of opinion and expression, of press and media, and of assembly and association. Vague definitions and provisions that grant broad discretionary power to the authorities in the application of the law may be misused to restrict access to information or suppress dissent. Accordingly, legislation designed to combat online violence must strike a delicate balance between protected interests to maintain order and prevent harm while also ensuring that individual rights and fundamental freedoms are not curtailed. Any restrictions must be necessary and proportionate, with clear identification and precise definitions of specific criminal behaviors in order to establish expectations for appropriate conduct and promote shared understanding of what constitutes a violation. The penalties delineated must also be necessary and proportionate, appropriate to the offense committed and sufficient for deterrence. The introduction of new criminal procedures to facilitate the investigation and prosecution of online violence – including those that relate to the detection of technology-enabled offenses and the access to, collection, retention, and management of digital evidence – must integrate appropriate safeguards to preserve individual rights to privacy and the protection of personal data, and regulate the powers granted to designated authorities to avoid government overreach.

In addition to defining offenses, delineating penalties, and outlining procedures for investigation and prosecution, legislation to address online violence must establish the primary status of victims and survivors as such, and stipulate the remedies, compensation, and support to which they are entitled on that basis. In some contexts, victims who have been subjected to certain forms of online violence, such as IBSA or CSAM, may be vulnerable to prosecution for their real or perceived complicity in the generation of these materials under applicable penal codes and criminal laws. Legislation on this topic should therefore function as a corrective to such risks, ensuring that survivors of profound violation are not disincentivized from reporting, are able to access needed protection, justice, and care in the aftermath of harm, and are treated first and foremost as victims in instances of potential liability. Additionally, legislation should detail the specific remedies to which survivors of online violence are entitled – such as physical protection and shelter care, information, legal counseling, medical assistance, mental health and psychosocial support, and compensation – and should establish clear reporting mechanisms and safe referral pathways through which survivors can access that care during the investigation, legal proceedings, and beyond.

Legislation to address online violence should also integrate provisions designed to prevent harm from occurring or reoccurring. These may include national education programs and awareness campaigns to build digital literacy, promote online safety practices, familiarize the public with common risks and dangers, and provide information on how to seek assistance. A law might also include initiatives to mitigate the conditions that facilitate and normalize online violence, or create disproportionate vulnerabilities for specific groups, by leveraging the role of media, schools, and relevant public institutions to challenge inequality, eradicate stereotypes, and promote mutual respect and pro-social conflict resolution strategies.[26] Regulatory obligations and accountability mechanisms for electronic service providers (ESPs) and technology companies should be established to ensure that devices are appropriately registered, age restrictions on devices and social media platforms are enforced, safety tools are available, content moderation protocols are enacted, and clear reporting mechanisms and take down procedures are in place.[27] Additional prevention measures that are particularly crucial to combating online violence against children include screening and training for those who work with children, as well as monitoring for offenders and those at risk of offending.

To build the institutional architecture required to leverage a comprehensive, end-to-end response to online violence, legislation should provide a clear framework that identifies all relevant agencies, defines their roles and responsibilities, and includes provisions to ensure that they are properly resourced and equipped to deliver on those obligations. This should include the establishment of a multi-stakeholder, cross-sectoral national body with authority to lead the overall response – ensuring harmonization and coherence with other national policies, strategies, and action plans; overseeing coordinated action across government, industry, and civil society; improving services and capacities within the country; monitoring and evaluating progress; and managing international cooperation, collaboration, and partnership to support an effective response to transnational crimes. It should also include the establishment of a dedicated law enforcement agency or unit with an explicit mandate to combat online violence and the requisite specialist knowledge and technical tools to conduct complex and sensitive investigations. Importantly, legislation should integrate provisions to ensure that all key agencies with a relevant mandate in the fight against online violence can benefit from systematic capacity-strengthening opportunities and specialized training programs, as well as a specifically allocated, adequate budget to facilitate implementation of their respective legal obligations.

26 In alignment with provisions of the Istanbul Convention, as well as precedents set by the Follow-up Mechanism to the Belém do Pará Convention (MESECVI) to develop a Model Law on TFGBV.

27 For a global standard on how legislation can regulate technology companies to incentivize safety by design, transparency, accountability, and responsibility, please see the STAR Framework (CCDH, 2022).

Recommendations

In Iraq and the Kurdistan Region, rapid technological advancements have expanded the frontiers of criminal activity, creating new risks for vulnerable groups and requiring adaptive policy solutions. Government stakeholders must take swift and concerted action to address the threat of online violence and preserve essential rights and protections in the digital dimension.

- The Government of Iraq (GOI) should ratify the United Nations *Convention Against Cybercrime*, reaffirming its commitment to combating online violence and demonstrating visionary leadership in addressing the particularly grave risks for women and children by assuming an international obligation to explicitly criminalize TF-CSEA and certain forms of TFGBV, such as the non-consensual distribution of intimate images, in its domestic legislation.

- The Governments of Iraq and the Kurdistan Region should thoroughly assess deficits in the current legislative environment, through a robust consultative process with diverse stakeholder groups, and enact new laws or amend existing laws to:
  - Create a strong, comprehensive legal framework for addressing online violations that includes measures to prevent violence, protect victims, prosecute perpetrators, and provide reparation to those affected;
  - Build the institutional architecture to leverage a coordinated, end-to-end response to online violence, including via designation of a leading agency or inter-agency body with an explicit legal mandate, and clear identification of other relevant institutions and their respective roles in implementation.

- In the absence of comprehensive legislation on this topic, the Governments of Iraq and the Kurdistan Region should abide by international legal standards and best practice – as encapsulated in the Council of Europe Budapest Convention, Lanzarote Convention, and Istanbul Convention[28] – in ongoing efforts to address online violence, and should strengthen enforcement of existing legislation in alignment with those frameworks.

28 Accession to these conventions is not necessary to benefit from their content, which may be used as a guideline, check list, or even as a model law to support the development of domestic legislation.