LEGISLATIVE ANALYSIS

ONLINE VIOLENCE IN IRAQ AND THE KURDISTAN REGION

AUTHORS

Adnan Qadir
Senior Legal and Advocacy Advisor

Kristin Perry
Senior Policy and Advocacy Advisor

Authors: Adnan Qadir and Kristin Perry

Date of Publication: August 2025

SEED is a women-led, local NGO in the Kurdistan Region of Iraq, working to create a future where everyone can thrive by protecting those at risk and advancing rights for all. We promote gender equality, protect children, combat human trafficking, and improve mental health and well-being. Through transformational services, community development initiatives, training and education programs, and advocacy, we support individuals, empower communities, and strengthen systems to create sustainable impact.

This analysis was produced with financial support from the United States Government and iQ Group. However, the opinions, findings, conclusions, and recommendations expressed herein are solely those of the authors.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY 5

2. PURPOSE 6

3. SCOPE 6

4. METHODOLOGY 6

5. LEGAL FRAMEWORK ON ONLINE VIOLENCE 7

5.1. INTRODUCTION 7

5.2. INTERNATIONAL LEGAL FRAMEWORK 8

5.2.1. The Council of Europe Convention on Cybercrime (Budapest Convention of 2001) 8

5.2.2 The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention of 2007) 10

5.2.3. The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention of 2011) 12

5.2.4. The Arab Countries Convention on Combating Information Technology Offenses (2010) 14

5.3. NATIONAL LEGAL FRAMEWORKS IN IRAQ AND THE KURDISTAN REGION 15

5.3.1. Iraqi Constitution of 2005 15

5.3.2. Iraqi Penal Code No. 111 of 1969 16

5.3.3. Law of Combating Trafficking in Persons No. 28 of 2012 in Iraq and No 6. of 2018 in the Kurdistan Region 17

5.3.4. Law on Preventing Misuse of Telecommunication Devices No. 6 of 2008 in the Kurdistan Region 18

5.3.5. Law of Combating Domestic Violence No. 8 of 2011 in the Kurdistan Region 21

5.3.5. Law of Combating Domestic Violence No. 8 of 2011 in the Kurdistan Region 21

5.3.6. Draft Law on Combating Cybercrimes in Iraq 21

5.4. REGIONAL LEGISLATIVE RESPONSES TO ONLINE VIOLENCE 24

6. INSTITUTIONS IN IRAQ AND THE KURDISTAN REGION 25

6.1. COMMUNICATIONS AND MEDIA COMMISSION IN IRAQ 26

6.2. MINISTRY OF INTERIOR IN IRAQ AND THE KURDISTAN REGION 26

6.2.1. Directorate of Combating Organized Crimes in the Kurdistan Region and Directorate of Combating Human Trafficking in Iraq 27

6.2.2. Directorate of Combating Violence Against Women and Families in the Kurdistan Region and Directorate of Protection of Women and Children in Iraq 27

6.3. MINISTRY OF LABOR AND SOCIAL AFFAIRS IN IRAQ AND THE KURDISTAN REGION 28

6.4. NATIONAL SECURITY AGENCIES IN IRAQ AND THE KURDISTAN REGION 28

7. KEY RECOMMENDATIONS AND PRIORITIES FOR LEGISLATION TO ADDRESS ONLINE VIOLENCE 28

GLOSSARY OF ACRONYMS

CMC	Communications and Media Commision
COE	Council of Europe
COR	Council of Representatives
CRC	Convention on the Rights of the Child
CSAM	Child Sexual Abuse Materials
CSEM	Child Sexual Exploitation Materials
CSO	Civil Society Organizations
DCOC	Directorate of Combating Organized Crimes
DCVAW	Directorate of Combating Violence Against Women and Families
EU	European Union
GOI	Government of Iraq
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organization
IQD	Iraqi Dinar
KRI	Kurdistan Region of Iraq
KRG	Kurdistan Regional Government
MENA	Middle East and North Africa
MOI	Ministry of Interior
MOLSA	Ministry of Labor and Social Affairs
NGO	Non-Governmental Organization
OPSC	Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography
SIM	Subscriber Identity Module
SMS	Short Message Service
TFGBV	Technology-Facilitated Gender-Based Violence
TF-CSEA	Technology-Facilitated Child Sexual Exploitation and Abuse
TIP	Trafficking in Persons
TY-C	Cybercrime Convention Committee
UN	United Nations
USD	United States Dollar

1. EXECUTIVE SUMMARY

In an increasingly digital world, online violence represents a pervasive threat to the safety and security of individuals, communities, and nations. In Iraq and the Kurdistan Region – where rates of violence are already high, fundamental protection frameworks are lacking, and social norms and cultural pressures can increase risks of honor-based stigma and reprisals for survivors – the consequences of online violence are especially profound. This is particularly true for members of vulnerable groups, including women and children. Women are disproportionately impacted by technology-facilitated gender-based violence (TFGBV),[1] an overarching term that encompasses diverse violations against women that are enabled or amplified through technology, while children are at alarming risk of technology-facilitated child sexual exploitation and abuse (TF-CSEA),[2] a distinct category of sexual offenses against children that involve the use of digital technologies.

Iraq and the Kurdistan Region face substantial challenges in addressing online violence, including TFGBV and TF-CSEA. Despite concerted action to combat these crimes within the confines of the extant legal framework, the absence of clear and coherent legislation on online violence has impeded institutional responses. The Iraqi Constitution, the preeminent and supreme law in the country, broadly prohibits violence, exploitation, and abuse – and the legislature has a responsibility to legislate within that framework. To date, however, the vast majority of applicable laws remain designed for traditional offenses, and may not be suitable to address online violations. Most do not explicitly identify and define key forms of online violence, mandate a specialized government agency to respond, or introduce appropriate technical procedures for the management of these crimes. Instead, the response to online violence is regulated via assorted provisions within an amalgam of general and specialized laws, with varying degrees of subject matter relevance and differing scopes of application – undermining clarity and coordination among responding institutions, resulting in inconsistent implementation, and leaving individuals at risk.

While the discourse on this topic continues to evolve in parallel with rapid technological advancements, and crafting legislation to address online violence can therefore be a daunting task, there are a number of international and regional instruments that can be used to support the development of strong domestic laws. Notably, the Council of Europe (COE) Budapest, Lanzarote, and Istanbul Conventions provide the most contemporary and comprehensive set of measures to tackle violence in the digital dimension, particularly against women and children. Legislators may use the common standards contained in these international agreements, along with their associated soft law provisions, as a guideline, checklist, or model law in efforts to create national legislation.

At the core of its approach to this issue, international law recognizes that instruments designed to regulate behaviors in the digital environment may be uniquely vulnerable to misapplication and abuse. It therefore seeks, through the integration of both substantive and procedural safeguards, to strike a delicate balance between protected interests – supporting the ability of national legislators to criminalize violence and other harms without infringing on fundamental rights and freedoms, including the rights to privacy and protection of data, as well as the freedoms of opinion and expression, of press and media, and of assembly and association. Additionally, international law recognizes that efforts to combat online violence must be comprehensive, extending beyond prosecution through the integration of measures to prevent violence, protect victims, provide remedy and reparation to those affected, and support a coordinated, multistakeholder and multisectoral response, including across borders on transnational crimes. Considering each of these components in the development of national legislation can provide an actionable roadmap to eradicating violence and keeping individuals safe online, enhancing the capacity of States to leverage an effective response.

This report analyzes the applicable legal framework in Iraq and the Kurdistan Region, including both general and specialized laws, against these benchmarks. As a comparative exercise, it also examines Kuwait's efforts to address online violence through the enactment of Law No. 63 of 2015 on Combating Information Technology Crimes – providing a salient regional example of a State integrating core global standards in a manner compatible with the local context and culture. After assessing some of the progress made and constraints faced by key government institutions working to combat online violence in the absence of a legal mandate, it concludes with recommendations to support the Government of Iraq (GOI) and the Kurdistan Regional Government (KRG) in developing legislation to address this growing threat.

1. Alternative terms like "cyberviolence against women" or "technology-facilitated violence against women" are used interchangeably in the literature and discourse to describe the same phenomenon. While TFGBV is used throughout this paper for consistency, it should be understood to maintain the common definition present across all terms, which relates to acts of violence against women and girls that are facilitated by technology.
2. The term online child sexual exploitation and abuse (OCSEA) is frequently used in the existing discourse on this topic, but the use of "technology-facilitated" as a central qualifier, rather than "online," is preferable to increase definitional accuracy and breadth, better reflecting the role of technology in enabling or amplifying these crimes against children in both online and offline contexts. 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.

It argues that a robust legislative response should, at a minimum:

- **Include Necessary Safeguards**. Recognizing that frameworks which criminalize behaviors in the digital environment are uniquely vulnerable to misapplication and abuse, and also recognizing that efforts to combat criminal activity can, if mismanaged, amplify risks for survivors, the law should provide necessary safeguards to govern all aspects of the response to online violence.
- **Establish a Comprehensive Approach**. To build a cohesive, integrated end-to-end response to online violence, the law should establish a comprehensive approach that includes measures for prevention, protection, prosecution, and reparation.
- **Build an Institutional Framework**. To operationalize the response to online violence, the law should provide a clear institutional framework, with mandated leadership and mechanisms to support multi-layered interventions and coordinated action across relevant stakeholders and sectors, for a strong "whole systems" approach.
- **Design for Impact.** To ensure the efficacy of the response to online violence, the law should include measures to support implementation, monitor and evaluate progress, and facilitate adaptation as needed.

2. PURPOSE

This analysis examines key international and national legal frameworks relevant to combating various forms of online violence, including TFGBV and TF-CSEA, in Iraq and the Kurdistan Region of Iraq (KRI). It stresses the importance of a balanced and comprehensive legislative response to combating online violence with a focus on prevention, protection, prosecution, reparation, and integrated policies. This analysis, developed by SEED, is informed by our first-hand experience as a provider of protection services in the KRI, that of other international and national non-governmental organizations (NGOs) and civil society organizations (CSOs), and recognized responses by government institutions across Iraq and the KRI. It concludes with key recommendations and priorities to inform the development of legislation to address online violence.

3. SCOPE

This legislative analysis offers a thorough examination of the key legal frameworks relevant to combating online violence in Iraq and the KRI. It does not provide an in-depth assessment of the intersecting legal precedents related to freedom of expression and free media.[3]

4. METHODOLOGY

This legislative analysis is heavily informed by a desk review of primary sources, including relevant laws and conventions governing the treatment of TFGBV and TF-CSEA within the framework of online violence, as well as available secondary sources. It is also informed by the experiences of SEED in the field, and supplemented by key informant interviews and other inputs from relevant stakeholders, where necessary.

3. The responsibility to preserve individual rights and freedoms must be taken into account when criminalizing online behaviors, and the regulation of such matters should balance protected interests and human rights. However, a detailed exploration of all relevant rights and freedoms is beyond the scope of this project. All recommendations related to the prevention, detection, and prosecution of online violence, as well as the protection of survivors, must be understood in that context, and are not intended to constrain the fundamental freedoms enshrined in Articles 38 and 40 of the Iraqi Constitution, as well as other national and regional laws.

5. LEGAL FRAMEWORK ON ONLINE VIOLENCE

5.1. INTRODUCTION

Online violence occurs in all public or private environments where individuals interact – which may include community, family, and personal spaces, workplaces, health facilities, educational settings, and more – and the redefinition of public and private spaces through technology-mediated environments.[4] There is currently no single internationally recognized definition of "online violence" as a standalone term. However, it is generally understood to refer to a broad array of harmful acts and behaviors that may be threatened, committed, facilitated, or aggravated through the use of information and communications technology (ICT).

In an increasingly digital world, online violence represents a pervasive threat to the safety and security of individuals, communities, and nations. As with offline forms of violence, however, those at greatest risk are often members of vulnerable groups, including women and children. Women are disproportionately impacted by TFGBV, an overarching term that encompasses diverse violations against women that are enabled or amplified through technology, including image-based abuse, sextortion, cyberstalking, cyberbullying, online harassment, online impersonation, defamation, hate speech, hacking, and doxxing. Children are at alarming risk of TF-CSEA, a distinct category of sexual offenses against children that involve the use of digital technologies, including subjection to sexual acts; coercion to perform sexual acts; the production, distribution, or possession of child sexual abuse materials (CSAM) or child sexual exploitation materials (CSEM); and the solicitation and grooming of children for these purposes. While TFGBV and TF-CSEA do not constitute an exhaustive list of potential violations against women and children in the digital dimension, they are emblematic of the unique dangers associated with technology-mediated environments, which are increasing in both prevalence and severity as technology continues to develop and proliferate.

The development of strong, comprehensive legislation is a key strategy in the fight against online violence. By addressing the unique manifestations of criminal activity in the digital sphere, designating a mandated institution or agency to respond, introducing specialized processes and procedures for detection and investigation, and providing an actionable roadmap to prevent violence, protect victims, prosecute perpetrators, and provide reparation to those affected, the enactment of legislation to address online violence can support the ability of States to leverage an effective and multifaceted approach to eradicating this significant threat.

The development, enactment, and implementation of legislation to address online violence is a process that must be managed with care and caution to avoid infringing upon the exercise of fundamental rights and freedoms in the digital dimension, including the right to privacy, and the freedoms of opinion and expression, of assembly, of press and media, and of communication and correspondence, among others. The responsibility of the State to preserve these rights and freedoms – as enshrined in Articles 38 and 40 of the Iraqi Constitution, applicable national and regional laws, and the relevant international frameworks to which Iraq is signatory[5] – must be taken into account when seeking to address online violence and harm, and the regulation of such matters should balance protected interests to mitigate risks of misapplication or abuse.[6]

4. General Recommendation No. 35 (UN Committee on the Elimination of Discrimination against Women, 2017).
5. Fundamental rights and freedoms are outlined in several important international frameworks to which Iraq is signatory, including the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), the International Covenant on Economic, Social, and Cultural Rights (1966), and other relevant instruments.
6. For more information on potential strategies to effectively address violations while preserving the enjoyment of human rights in the digital world, see a suggested set of principles from the Alliance for Universal Digital Rights (AUDRi) to advance an open, free and secure digital future for all via the Global Digital Compact, available here.

5.2. INTERNATIONAL LEGAL FRAMEWORK

Generally, at the core of its approach to this issue, international law seeks to reconcile the vision of a free internet, where information can be accessed and shared freely, with a robust criminal justice response to combating online violence. The common understanding behind these frameworks is that any restriction on fundamental rights must be proportionate and necessary, and that those restrictions must be narrowly defined, precisely specifying criminal behaviors and ensuring that prosecution and investigation are subject to rule of law safeguards and due process.

In this regard, the State has two facets of responsibility: first, the State, through its authorities and institutions, must respect the law and refrain from wrongful acts; and second, the State must exercise due diligence and protect individuals from non-State actors. This obligation is not an obligation of result, but an obligation of means, which requires the State to put effort into organizing its response to human rights violations. In both cases, failure to do so will incur State responsibility.

There are several relevant international instruments that provide the most contemporary and comprehensive set of measures to prevent and combat online forms of violence, particularly against women and children, and provide appropriate remedies for survivors. These measures provide standards and guidance to support national legislators in identifying and defining online violations and introducing special procedures to effectively investigate and hold perpetrators accountable for criminal behaviors.

The Council of Europe (COE) Budapest Convention, Lanzarote Convention, and Istanbul Convention are the most relevant international agreements that provide common standards applicable to combating online violence. The provisions are sufficiently precise to meet rule of law standards, but flexible enough to permit adaptation to different legal systems in any region of the world.[7] Moreover, in parallel to the evolution of technology, these instruments can be dynamically adapted through the establishment of soft law provisions by their corresponding group experts and specialized committees. The Arab Countries Convention on Combating Information Technology Offenses (2010) is the regional instrument for Arab countries, and is particularly relevant to this discussion as Iraq has ratified it. Therefore, all four instruments will be analyzed.[8]

5.2.1. THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION OF 2001)

The Council of Europe Convention on Cybercrime[9] (hereafter referred to as the Budapest Convention) is the most comprehensive international instrument on cybercrimes and electronic evidence. The Budapest Convention was developed by the COE and other non-European states in 2001, entered into force in 2004, and has been ratified by 80 countries around the globe. The Convention provides a global legal framework to support parties in developing domestic legislation to define the various behaviors that constitute cybercrime, ranging from illegal access, data, and systems interference to computer-related fraud and child pornography.[10] The Budapest Convention also introduces procedural techniques and tools to investigate cybercrime, ensuring the safety and security of electronic evidence. It also serves as a legal basis for international cooperation in addressing cybercrime among state parties to the Convention. The Convention is supplemented by its first protocol on cybercrime, which concerns the criminalization of acts of a racist and xenophobic nature committed through computer systems,[11] and a second additional protocol on enhanced co-operation and disclosure of electronic evidence.[12]

The Budapest Convention established the Cybercrime Convention Committee (T-CY) to assess the implementation of the Convention, exchange information, and share good practices. The specialized Cybercrime Programme Office of the COE leads on capacity building for parties to the Convention and provides technical assistance to support the integration of substantive and procedural standards into domestic laws.

It is essential to note that the Budapest Convention reconciles the vision of a free internet, where information can flow freely and be equitably accessed and shared, with the need for an effective criminal justice response in cases of criminal misuse. Restrictions are narrowly defined, and only specific criminal offenses are investigated and prosecuted. Data that is needed as evidence in specific criminal proceedings is subject to rule of law safeguards.

7. 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, provide valuable benchmarks for addressing the threat of online violence against women and children, and may be used as a guideline, check list, or even as a model law to support the development of domestic legislation.
8. NB: In December 2024, the United Nations formally adopted a new Convention against Cybercrime, which seeks to enhance international cooperation and establish a unified legal framework to address the escalating threats posed by digital crimes. An examination of this new framework, which requires ratification by 40 signatories to enter into force, is beyond the scope of this analysis. Nevertheless, the adoption of this convention represents a significant step forward in global efforts to combat cybercrime.
9. Convention on Cybercrime (Council of Europe, 2001).
10. Although child pornography is the legal term used in this convention and other laws referenced throughout this piece, the terms child sexual abuse material (CSAM) and child sexual exploitation material (CSEM) have become more widely used to reflect the inherently abusive and exploitative nature of this grave offense against children.
11. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Council of Europe, 2003).
12. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Council of Europe, 2022).

BUDAPEST CONVENTION IN RELATION TO ONLINE VIOLENCE

The Budapest Convention and its additional protocols, particularly when placed in conversation with the Istanbul and Lanzarote Conventions, offer a strong framework to combat online and technology-facilitated violence against women and children and fulfill their rights in the digital environment. In general, the Budapest Convention criminalizes offenses perpetrated against or by means of computer data and systems, and calls for specific procedural laws to strengthen investigation, prosecution of perpetrators, and the preservation of electronic evidence. The applicability of these provisions to specific forms of online violence may vary.

However, in 2018, the T-CY's Working Group on Cyberbullying and Other Forms of Online Violence Especially against Women and Children published a mapping study on cyberviolence to examine the applicability of the framework to violence facilitated by technology.[13] The T-CY broadly defines cyberviolence as potentially involving "different types of harassment, violation of privacy, sexual abuse and sexual exploitation and bias offences against social groups or communities," and notes that "cyberviolence may also involve direct threats or physical violence as well as different forms of cybercrime."[14]

Substantive Law

Through a number of substantive criminal law provisions, the Budapest Convention also directly and indirectly addresses several types of online and technology-facilitated violence. Articles 2-13 of the Convention are designed to improve the means to prevent and suppress computer (or computer-related) crimes by establishing a common minimum standard of relevant criminal offenses. Some of these provisions have direct relevance to forms of TFGBV and TF-CSEA, or facilitate important connections to them.

Article 4 of the Budapest Convention stipulates that data interference is the intentional damaging, deletion, deterioration, alteration, or suppression of computer data without right. In terms of common forms of online violence against women and children, this article could potentially be applied to manifestations like image-based abuse, which might entail deleting a photo on a gallery or editing a post on Facebook. It could also relate to the manipulation of photos or the development of deep fakes without the consent of the person who owns the data. Article 5 stipulates that system interference is intentionally hindering the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data without right. With regards to TFGBV, Article 5 could potentially be applied to a data breach that compromises women's safety, or the installation of stalkerware on a victim's device in order to monitor technology use and transmit activity data. Article 9 criminalizes producing child pornography for the purpose of distribution via computer, procuring child pornography via computer, and making child pornography available and/or distributing and transmitting it via computer. The digital production, procurement, and/or distribution of child pornography (also known as CSAM) is a form of TF-CSEA.

In terms of provisions that facilitate broader connections to online violence, Article 2 of the Budapest Convention criminalizes intentional and illegal access to the whole or any part of a computer system without right. A common example of illegal access is hacking, which is not only a recognized form of TFGBV in its own right, but is also implicated in many other forms of TFGBV, including cyberthreats, cyberstalking, and sextortion. Article 3 defines illegal interception as the interception without right, made by technical means, of non-public transmissions of computer data to, from, or within a computer system. In this form, incoming and outgoing communications of a victim may be intercepted, such as via tapping. Illegal interception may also be utilized in the context of privacy violations like those described above. The alteration of social media posts to attract or inspire hostility amounts to data interference, as per Articles 4 and 5.[15] Article 6 covers the misuse of a device for the intentional commission of a crime. For example, a perpetrator may break into a school system to harvest passwords and then use it to transmit cyberthreats as a form of TFGBV.

Procedural Law

Beyond substantive law provisions, the Budapest Convention also introduces some procedural rules to be incorporated into domestic laws. These procedural rules, which are designed to prevent cyberviolence in all forms, offer state parties robust measures to apply to criminal investigations and proceedings in individual cases of online violence. Articles 16 and 17 provide measures on the expedited preservation and partial disclosure of data. The competent authorities of state parties to the Budapest Convention, under the supervision of the judiciary,

13. Mapping study on cyberviolence (Council of Europe T-CY, 2018).
14. Ibid.
15. Articles 4 and 5, therefore, both have direct relevance to TFGBV and facilitate important connections to it.

may order the preservation of existing stored data and the disclosure of such data by data holders and service providers in relation to specific criminal investigations or proceedings. Article 18 provides that the competent authorities may compel a person within their territory to provide existing or stored data, and may compel a service provider operating within the territory to submit subscriber information. Subscriber information that service providers may be compelled to disclose, based upon an order from the competent authorities, can include the type and duration of communication service used, as well as the subscriber's identity, address, and telephone numbers that may be available on the basis of the service agreement or arrangement.

In addition to existing measures related to the search and seizure of tangible objects in criminal procedural laws, Article 19 provides contemporary measures on the search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. These measures empower the competent authorities to access and search computer data, within a computer system or part of it, or in an independent data storage medium, such as a disk. The competent authorities may also seize or similarly secure a computer system or part of it, or a data storage medium, and create a copy of its data. Articles 20 and 21 of the Budapest Convention provide that the competent authorities are to be empowered to collect and record traffic data and content data associated with specified communications transmitted by a computer system. The authorities may also compel a service provider, within its technical capacity, to cooperate and assist with the recording and collection of the above mentioned data. As content data may have a higher level of privacy protection, some domestic laws impose greater limitations on the recording and collection of such data, depending on the nature of the content or message being communicated.

Finally, Article 23 of the Budapest Convention requires that all parties cooperate, to the greatest extent possible, on investigations or criminal proceedings related to computer systems or data. This also applies to cases of extradition, which is especially crucial as perpetrators of online violence can, and do, perpetrate crimes remotely. Overall, given the procedural powers outlined, the Budapest Convention presents a strong legal framework for responding to cases of online violence and pursuing justice for survivors. However, to provide a complementary lens on the specific vulnerabilities faced by women and children, and add greater depth to existing criminal offenses, it should be placed in conversation with the Lanzarote and Istanbul Conventions, and bolstered by the enactment of national-level legislation to protect children and combat violence against women.

5.2.2 THE COUNCIL OF EUROPE CONVENTION ON THE PROTECTION OF CHILDREN AGAINST SEXUAL EXPLOITATION AND SEXUAL ABUSE (LANZAROTE CONVENTION OF 2007)

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[16] or Lanzarote Convention, was adopted in 2007 and entered into force in 2001. It has been signed and ratified by all COE member states, as well as acceded to by other countries. The Lanzarote Convention is the first regional treaty specifically focused on protecting children from sexual violence, and is also the first international legal instrument to criminalize the act of grooming. It takes a comprehensive approach to combating sexual offenses against children, including measures for prevention, protection, prosecution, and the promotion of national and international cooperation in addressing these crimes. Key prevention measures include education and awareness initiatives for children, screening and training for those in contact with children, and monitoring and intervention programs for offenders and potential offenders. For protection, the convention stipulates the establishment of reporting mechanisms and helplines, child-friendly judicial proceedings, and programs to provide victim support and assistance, including therapeutic measures and emergency psychological care. The prosecution parameters of the convention criminalize a specific set of acts that constitute sexual violations against children, while the emphasis on cooperation in addressing these crimes encourages states to adopt nationwide, integrated policies to support coordinated and effective action, and to participate in information exchange and collaborative identification of solutions with international stakeholders to combat impunity for transnational crimes. This convention is designed to be fully compatible with – and complementary to – the United Nations (UN) Convention on the Rights of the Child (CRC) and its optional protocols, including the Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography (OPSC).[17]

16. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Council of Europe, 2007).

17. For broader treatment of the protection and rights of children, including in the digital dimension, please see the United Nations Convention on the Rights of the Child (CRC), its optional protocols, and General Comment No. 25 of 2021 (CRC/C/GC/25), issued by the Committee on the Rights of the Child, on how States parties should apply the provisions of the CRC in the digital context. Iraq is signatory to the CRC and several of its optional protocols, including the Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography (OPSC), which obliges State Parties to criminalize and prevent all forms of child sexual exploitation and abuse – including the use of children in pornography, sexual performances, and child sexual exploitation and abuse materials – and to align national legislation with the protocol's provisions. The Lanzarote Convention is fully compatible with these key frameworks.

LANZAROTE CONVENTION

Within its prosecution pillar, the Lanzarote Convention criminalizes a number of sexual offenses against children, including:

- Child sexual abuse: which refers to any sexual activities with a child who has not reached the legal age for those activities, or activities in which a vulnerable situation or position of trust and authority is abused, or in which coercion, force, or threats are used;
- Child prostitution:[18] which encompasses any situation where a child is recruited, coerced, or otherwise caused to participate in prostitution in exchange for money or other benefits, or in which a person has recourse to – or profits from – the exploitation of children for such purposes;
- Child pornography: which refers to any material that depicts a child engaged in real or simulated sexually explicit conduct or depicts a child's sexual organs for primarily sexual purposes, and includes the production, offering, distribution, procurement, and possession of such materials, or intentional access to them;
- Participation of a child in pornographic performances: which involves any situation where a child is recruited, coerced, or otherwise caused to participate in such performances, or in which a person profits from or knowingly attends such a performance;
- Corruption of children: which refers to the act of intentionally causing a child who has not reached the legal age for sexual activities to witness sexual activities or sexual abuse for sexual purposes;
- Solicitation of children for sexual purposes (also known as "grooming"): which refers to an adult intentionally proposing, through ICTs, to meet with a child who has not reached the legal age for sexual activities for the purpose of committing any of the above offenses, followed by material acts leading to such a meeting;
- Any act to intentionally aid or abet the commission of these offenses, and any intentional attempts to commit them.

This legal instrument has been harmonized with the Budapest Convention through the Lanzarote Committee's Interpretative Opinion[19] on the applicability of the Lanzarote Convention to sexual offenses against children facilitated through the use of information and communication technologies (ICTs), and a subsequent Declaration on protecting children against sexual exploitation and sexual abuse facilitated by emerging technologies.[20] These supplemental resources recognize that ICTs have created new avenues for sexual offenders to exploit and abuse children, establish the applicability of the Convention to these offenses, and call upon State Parties to take needed measures to protect children from acts of sexual exploitation and abuse committed via these means. Therefore, because the offenses defined in the Lanzarote Convention apply in the same manner, regardless of whether perpetrators use ICTs or other methods to commit those offenses, the Lanzarote Convention offers an important framework for addressing TF-CSEA, a key form of online violence against children.[21]

18. "Prostitution" is the legal term used in the text of this convention and in other laws referenced throughout this piece. 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.
19. Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offenses against children facilitated through the use of information and communication technologies (ICTs) (Council of Europe Lanzarote Committee, 2017).
20. Declaration on protecting children against sexual exploitation and sexual abuse facilitated by emerging technologies (Council of Europe Lanzarote Convention, 2024).
21. NB: The Cybercrime Convention Committee (T-CY) has also affirmed that the Lanzarote Convention and the Budapest Convention are complementary. Consequently, any acts of online violence that are not specifically covered by the Lanzarote Convention can be addressed and criminalized under the Budapest Convention, which deals directly with cybercrime and the use of technology in committing violence. See the T-CY's Mapping Study on Cyberviolence and the COE's ongoing work to address Cyberviolence Against Children for more information.

5.2.3. THE COUNCIL OF EUROPE CONVENTION ON PREVENTING AND COMBATING VIOLENCE AGAINST WOMEN AND DOMESTIC VIOLENCE (ISTANBUL CONVENTION OF 2011)

The COE adopted the global Convention on Preventing and Combating Violence against Women and Domestic Violence, or Istanbul Convention, in 2011, which entered into force in 2014 and has been signed by all European Union (EU) member states and acceded to by other parties, including the EU. The Convention introduces a comprehensive and holistic response to multiple forms of violence, and sets out significant obligations for state parties to establish protection and support services. The Istanbul Convention includes four key pillars: prevention, protection, prosecution, and coordinated policies. The prevention pillar promotes positive change in social norms, awareness raising and education, women's empowerment, and men and boys' engagement. The protection pillar seeks to ensure that survivors are protected, receive adequate information, and have access to needed support services, including legal and psychological counseling, financial and job assistance, housing, education, and training. The prosecution pillar is designed to preserve the rights of survivors and hold perpetrators accountable for wrongdoing through effective legislative, judicial, and law enforcement responses. The final pillar, focused on coordinated policies, is designed to provide comprehensive and rights-based policies, allocate needed financial resources, and ensure coordination between relevant actors and agencies, both governmental and non-governmental, to support a whole systems approach to preventing and combating violence.

The Convention provides a comprehensive definition of violence against women by recognizing the broad-ranging forms that such violence can take, comprising all acts "that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life."[22] It also provides a definition of domestic violence that covers acts of physical, sexual, psychological, or economic violence between members of the family. The due diligence principle is enshrined in the Istanbul Convention and is designed to prevent, investigate, punish, and provide reparation for acts of violence.

ISTANBUL CONVENTION IN RELATION TO ONLINE VIOLENCE

The Convention set up a Group of Experts on Action against Violence against Women and Domestic Violence (hereafter "GREVIO") to monitor the implementation of the Convention and adopt general recommendations. These recommendations are not legally binding; however, they compose a significant part of the soft law and provide interpretive guidance for articles included in the Convention. In 2021, GREVIO adopted its first General Recommendation on the digital dimension of violence against women.[23] This recommendation underscores the lack of direct references to online violence in the Istanbul Convention, but serves to reinforce it as an expression of violence that is covered by the Convention. GREVIO considers online violence a key dimension of violence against women and establishes, therefore, that the definition contained in the Istanbul Convention is applicable to – and inclusive of – common types of TFGBV, including non-consensual image and video sharing, bullying, online sexual harassment, online stalking, and psychological abuse perpetrated via digital means. While there are many different methods of categorizing and classifying the various acts that constitute TFGBV based on the relationship between the survivor and the perpetrator, the behavioral modalities of abuse, and the means of perpetration, offenses falling within the broader definitions of online sexual harassment, online stalking, and online psychological violence appear to be most immediately compatible with the Istanbul Convention.

22. Convention on Preventing and Combating Violence Against Women and Domestic Violence (Council of Europe, 2011).
23. GREVIO General Recommendation No. 1 on the digital dimension of violence against women (Council of Europe GREVIO, 2021).

Online Sexual Harassment:

Article 40 of the Istanbul Convention stipulates that sexual harassment comprises "any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment."[24]

The European Union Agency for Fundamental Rights defines online sexual harassment as "unwanted sexually explicit emails or SMS messages that offend, inappropriate advances that offend on social networking websites such as Facebook, or in internet chat rooms."[25] GREVIO, in its General Recommendation No. 1 on the digital dimension of violence against women, states that the following behaviors fall under the remit of Article 40 of the Convention:

- Non-consensual image or video sharing, which covers sharing of nude or sexual photos and videos of a person without her/his consent (also called image-based sexual abuse or revenge pornography).
- Non-consensual taking, producing, or procuring of intimate images or videos, which includes "creepshots," "upskirting," and "deepfaking." "Creepshots" involve taking a sexual or private picture of a person without consent. "Upskirting" is taking a sexual picture of a person under their dress without consent. "Deepfaking" is replacing one face with another in a video or an image.
- Exploitation, coercion, and threats, which include forced sexting, sexual extortion, rape threats, doxxing, and impersonation.
- Sexualized bullying, which includes any act of spreading gossip or rumors about the sexual behavior of a person, writing sexualized comments on someone's photos or posts, and impersonating someone to share sexual content or harass others.
- Cyberflashing, which includes sending sexual pictures through dating or message applications, texts, or using AirDrop or Bluetooth technologies.

Online and Technology-Facilitated Stalking:

Article 34 of the Istanbul Convention provides that stalking is "intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety." The explanatory report of the Convention provides that "this includes physically going after the victim, appearing at her or his place of work, sports or education facilities, as well as following the victim in the virtual world (chat rooms, social networking sites, etc.)."[26]

Online Psychological Violence:

Article 33 of the Istanbul Convention urges states to criminalize all forms of psychological violence, outlining psychological violence as "the intentional conduct of seriously impairing a person's psychological integrity through coercion or threats." In General Recommendation No. 1, GREVIO explains that all forms of technology-facilitated violence have psychological impact on – and implications for – survivors. In domestic violence cases, offline forms of psychological violence can transform to radical new manifestations with the assistance of technology. For example, domestic violence can take on a new dimension when current or former partners are in possession of a survivor's intimate images.

In summary, the Istanbul Convention defines violence against women and domestic violence in both offline and online forms, and sets the highest standard for addressing those violations within international law. TFGBV consists of a wide range of behaviors and forms of online violence that fall under the definition of violence against women set out in the Istanbul Convention. Additionally, the Istanbul Convention introduces four pillars on prevention, protection, prosecution, and coordinated policies, which, taken together, comprise a comprehensive and holistic approach to combating TFGBV. It also assists state parties in developing effective response mechanisms to address all aspects of violence against women and domestic violence. The available protections in the Istanbul Convention should be complemented by other relevant instruments that are specifically designed to combat online violence, such as the Budapest Convention.

24. Convention on Preventing and Combating Violence Against Women and Domestic Violence (Council of Europe, 2011).
25. For more information, see: PROTECTING WOMEN AND GIRLS FROM VIOLENCE IN THE DIGITAL AGE (Council of Europe, 2021).
26. The Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence (Council of Europe, 2011).

5.2.4. THE ARAB COUNTRIES CONVENTION ON COMBATING INFORMATION TECHNOLOGY OFFENSES (2010)

In December 2010, the Interior and Justice Ministries of the Arab States signed the Convention on Combating Information Technology Offenses (hereafter referred to as the Arab Countries Convention) to protect the security and interests of the Arab States and the safety of their communities and individuals. The Arab Countries Convention mainly covers substantive provisions to define information technology terms and offenses, procedural provisions to investigate these offenses, and cooperation between the Arab States in combating such offenses. Ratifying the Arab Countries Convention creates an international obligation to incorporate the provisions of the Convention into the domestic legislation of state parties. Iraq ratified the Arab Countries Convention by the Law of Ratification of the Convention on Combating Information Technology Offenses No. 31 of 2013.

The provisions of the Arab Countries Convention are almost the same as those of the Budapest Convention in terms of substantive rules, procedural powers, and international cooperation. However, the Budapest Convention clearly reiterates the importance of balancing a robust criminal justice response to cybercrime with the responsibility to protect civil liberties. In particular, the Budapest Convention emphasizes individual rights, such as the right to freedom of opinion and expression, including the freedom to seek, receive, and impart information, as well as the right to privacy stipulated within the International Covenant on Civil and Political Rights (ICCPR) in 1966, the CRC in 1989, and other international instruments. By contrast, the Arab Countries Convention focuses primarily on the safety, security, and interests of states, although it does briefly reference international human rights in the preamble. This overall approach is clearly observed throughout the Arab Countries Convention, which incorporates a section on offenses related to terrorism and organized crime committed by means of information technology, as well as one on cybercrimes related to the safety and security of state parties. Iraq adopted a similar approach in the Law of Ratification of the Convention on Combating Information Technology Offenses No. 31 of 2013, reaffirming the need to protect the safety, security, and interests of the state in the founding reasons of the law.

The Arab Countries Convention criminalizes certain information technology acts in Articles 5 to 21. The offenses listed include illegal access, illegal interception, offenses against the integrity of data, misuse of information via technological means, forgery and fraud, pornography, offenses against privacy, offenses related to terrorism committed by means of information technology, offenses related to organized crime committed by means of information technology, violations of copyright and adjacent rights, and the illicit use of electronic payment tools.

With the exception of the section on offenses related to terrorism[27] and organized crime, the criminalized acts in the Arab Countries Convention, like those in the Budapest Convention, either have direct relevance to online violence or facilitate important connections to it. While the criminalization of such behaviors is a positive step toward the protection of survivors of violence and those at risk, the emphasis on state interests over individual human rights reflects the potential for the prioritization of the State over the safety and wellbeing of citizens in the application of the Arab Countries Convention. Additionally, the Arab Countries Convention has not been harmonized as effectively with other relevant frameworks for the protection of women and children in the digital environment.

27. It is important to note that, in an increasingly digital world, online violence and other forms of crime are not always clearly circumscribed nor mutually exclusive. For instance, ISIS using Facebook and WhatsApp to sell Yezidi women into sexual slavery is not only an example of TFGBV, but is also an act of both trafficking and terrorism, as conflict-related sexual violence has been recognized as a constituent element of war crimes, crimes against humanity, and genocide.

5.3. NATIONAL LEGAL FRAMEWORKS IN IRAQ AND THE KURDISTAN REGION[28]

Iraq and the KRI do not have clear and coherent legislative frameworks for combating online violence. Instead, online violence is regulated via an amalgam of general and specialized laws, with varying degrees of subject matter relevance and different scopes of application.[29] This can undermine institutional clarity, coordination, and accountability around relevant legal responsibilities, resulting in inconsistent implementation and impeding the ability of the GOI and KRG to leverage an effective and comprehensive response to specific threats, such as TFGBV and TF-CSEA.

While executive government agencies have, at times, sought to address such gaps via the issuance of regulations and instructions, the authority to determine criminal behaviors and appropriate punishments for such behavior must only be exercised by the legislature, and any attempt to do so by an executive agency, under any name, is unconstitutional.[30]

Importantly, the criminalization of online acts and offenses can run the risk of compromising essential rights and freedoms in the digital dimension, including the right to privacy, the right to hold an opinion, freedom of expression, freedom of the press, media, and publications, and so forth. Therefore, penal and procedural codes regulating these matters should balance between protected interests.

This section briefly touches upon the existing legal framework in Iraq and the KRI related to fundamental rights and freedoms, before analyzing applicable laws related to the criminalization of violence in the digital dimension.

5.3.1. IRAQI CONSTITUTION OF 2005

The Iraqi Constitution is the supreme law of the land that establishes individual rights and available protections. Since its issuance in 2005, however, new technologies and means of communication have proliferated in Iraq and, as a significant proportion of social interaction increasingly takes place online, new manifestations and types of violence have begun to emerge in the digital sphere. It is essential to note that any measures to combat TFGBV and TF-CSEA, in alignment with constitutional prohibitions on all forms of violence and abuse, must also consider the human rights standards enshrined within the same framework. From this perspective, the criminalization of any behavior must be necessary, proportional, and not contradict the core of one or more protected rights and freedoms.

IRAQI CONSTITUTION OF 2005

In Article 38, the Constitution states:

The State shall guarantee in a way that does not violate public order and morality:

First: Freedom of expression using all means.

Second: Freedom of press, printing, advertisement, media and publication.

Third: Freedom of assembly and peaceful demonstration, and this shall be regulated by law.

It also stipulates, in Article 40, that:

[...] the freedom of communication and correspondence, postal, telegraphic, electronic, and telephonic, shall be guaranteed and may not be monitored, wiretapped, or disclosed except for legal and security necessity and by a judicial decision.

Given that the freedoms of expression, of press and media, and of communication and correspondence all have digital dimensions, these essential protections must be taken into account when criminalizing online behaviors.

In terms of combating harms, the Constitution prohibits, in Article 29/4, *"all forms of violence and abuse in the family, school, and society."* It also provides that *"economic exploitation of children in all of its forms shall be prohibited and the State shall take the necessary measures for their protection"* (Article 29/3) and that *"forced labor, slavery, slave trade, trafficking in women or children, and sex trade shall be prohibited"* (Article 37/3). These broad provisions encompass numerous forms of violence, exploitation, and abuse, whether occurring offline or online. It is the responsibility of the legislature to legislate appropriate laws within the framework of the Constitution.

28. Iraq is a federal state and the provisions of the Iraqi Constitution apply in all parts of Iraq. However, other federal laws may not be applicable in the KRI unless they fall within the enumerated powers of the federal government, are adopted by the KRG, or predate its legislative independence (as established by Decree No. 11 of 1992).
29. Applicable criminal frameworks include the Iraqi Penal Code, the primary law regulating criminal behaviors, and a number of specialized laws on specific categories of offenses, such as trafficking, prostitution, domestic violence, and so forth. The vast majority of applicable laws were designed to govern the management of traditional offenses, and are missing core components that would make them suitable for use in the digital age. While they 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, these frameworks were not designed for use in the digital age and 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.
30. See Articles 19/2 and 61/1 of the Iraqi Constitution of 2005.

As part of this process, legislators must consider constitutional rights and freedoms when designing laws to combat online violence and exploitation, including TFGBV and TF-CSEA. Substantive and procedural measures must be proportional and necessary. Criminal behaviors must be narrowly specified so that individuals know what is prohibited in advance. Criminal procedures, among other things, must ensure the integration of due process and fair trial standards, and prevent illegal intrusion on individual rights. Moreover, the prescribed punishments for each form of TFGBV and TF-CSEA must be proportional and sufficient to deter perpetrators from committing online violence again.

5.3.2. IRAQI PENAL CODE NO. 111 OF 1969

In the absence of laws specifically designed to combat online violence, the Iraqi Penal Code No. 111 of 1969 is the primary applicable law that applies to criminal behaviors, although some of its provisions may be secondary to those found within other specialized laws, including the frameworks subsequently examined in this section.[31]

IRAQI PENAL CODE NO. 111 OF 1969

There are a number of general provisions in the Iraqi Penal Code that apply to various forms of online violence. Section 5, Part 7 defines criminal conduct related to cable and wireless communications. Article 363 stipulates that *"any person who willfully upsets others by the misuse of cable or wireless communication equipment is punishable by a period of detention*[32] *not exceeding 1 year plus a fine not exceeding 225,000 IQDs or by one of those penalties."*

The Iraqi Penal Code also regulates some forms of online violence through provisions related to threats, defamation, insult, and the disclosure of secrets throughout Articles 430-438, as well as acts of indecency and sexual offenses against children in Articles 393-403, which can be interpreted to apply to violations committed by online means. In Article 430, the Penal Code states that *"any person who threatens another with the commission of a felony against his person or property, or against the person or property of others, or with the imputation to him of certain dishonorable matters, or with the revelation of such matters, and such threat is accompanied by a demand or charge to carry out or refrain from carrying out an act, or is intended to be so accompanied, is punishable by a term of imprisonment not exceeding 7 years or by detention."*

It also provides, in Article 432, that *"any person who threatens another by word or action or in a written or spoken reference, or through another person, or in circumstances other than those mentioned in Articles 430 and 431 is punishable by a period of detention not exceeding 1 year or by a fine not exceeding 225,000 IQDs."* In Article 433/1, the Penal Code states that *"defamation is the imputation of a certain incident to another via a public method which, if true, would expose such a person to punishment or cause him to be scorned by society."* It also stipulates, in Article 434, that *"insulting is the imputation to another of something dishonorable or disrespectful, or the hurting of his feelings, even though it does not include an imputation to him of a particular matter."* Defamation and insult are punishable by detention and a fine, either combined or as separate punishments. If defamation or insult is published in a newspaper, publication, or other press means, it is considered an aggravating circumstance[33] and the punishment increases accordingly.

31. The application of the latter is in line with an established principle in criminal justice that the provisions of a new and/or specialized law shall supersede the provisions of an existing and/or general law when those laws are in conflict.
32. NB: The Penal Code, in Articles 87-89, defines three tiers of penal confinement that vary in severity and duration, including imprisonment (alsijn), whether for life or a period between 5 and 15 years, and detention (alhabs) that can be either severe (not less than 3 months and not exceeding 5 years unless otherwise stipulated, including a penal servitude or prison labor component when the duration of detention is more than 1 year) or simple (no less than 24 hours and not exceeding 1 year unless otherwise stipulated, with no penal servitude or prison labor component). While all terms refer to penal confinement, "imprisonment" and "detention" are used throughout this piece, in English, to denote the use of "alsijn" and "alhabs," respectively. The use of the term "detention" in this piece is not to be confused with "altawqif," as referenced in Articles 109-120 in the Criminal Procedural Law No. 23 of 1971.
33. See Articles 433 and 434 of the Penal Code.

Article 435 provides that, *"if the defamation or insulting is directed at the victim in private or via a telephone conversation, or if it is sent to the victim in writing or communicated to him by other means, the penalty will be a period of detention not exceeding 6 months plus a fine not exceeding 225,000 IQDs or by one of those penalties."*

In regard to the disclosure of the personal and family secrets of an individual, Article 437 states that *"any person who, by reason of his office, profession, trade or the field of nature of her/his work, is privy to confidential information and who discloses such information in circumstances other than those prescribed by law or uses it to his advantage or to another person's advantage is punishable […]."* Furthermore, Article 438 provides that *"any person who publishes, in any way, a picture, remark, or information in respect of the private or family life of another, even though such information is true, if such publication causes him offense"* and *"any person*[34] *[…] who is privy to information contained in a letter, telex, or telephone conversation and he discloses such information to a person other than for whom it is intended and such disclosure causes harm to another, is punishable by detention […] and fine […] or one of those punishments."*

Articles 400 and 401 of the Iraqi Penal Code criminalize acts of indecency. If such acts are committed publicly, the penalties are more severe. Articles 402 and 403 criminalize actions such as *"requesting indecent things from a male or female or exposing a female in a public place with words, actions or gestures in a way that offends her modesty and the creation, possession and transportation of indecent materials."* These provisions could be interpreted to apply to offline and online violations equally.

Articles 396 and 397 criminalize the consensual and non-consensual sexual assault of children, with or without the use of threat, coercion, or deception. Article 399 states that *"any person who incites a boy or girl under the age of 18 to indulge in fornication or resort to prostitution as a profession or assists him or her to do so is punishable by detention. The penalty will be a term of imprisonment not exceeding 10 years or by detention if the offender […] intends to profit by his action or receives money for such action."*

The above provisions of the Iraqi Penal Code – including on the misuse of communication devices to upset others; threat, insult, defamation, disclosure of secrets; indecent acts and materials; and sexual offenses against children – can be applied to numerous forms of TFGBV and TF-CSEA. However, there are a number of shortfalls and challenges when it comes to the implementation of these provisions for TFGBV and TF-CSEA crimes. The law does not clearly define these forms of online violence; rather, all forms of TFGBV and TF-CSEA are regulated in a few articles, and under broad definitions. These provisions remain general for the purpose of implementation, which grants significant discretionary authority to the judiciary to address a vast range of online activities within this scope, leading to different judicial interpretations of these general provisions. In fact, the judiciary can broadly interpret several of the listed provisions to prosecute an individual for criticism of the government. Such broad definitions also risk creating confusion among members of the public about what is considered a crime and what is protected within the scope of freedom of expression.

5.3.3. LAW OF COMBATING TRAFFICKING IN PERSONS NO. 28 OF 2012 IN IRAQ AND NO 6. OF 2018 IN THE KURDISTAN REGION

The Law of Combating Trafficking in Persons was enacted in Iraq in 2012 and subsequently adopted by the Kurdistan Region in 2018.

34. When the person is an official or employee in a postal or telecommunications agency, or a public official or agent, the punishment increases according to Article 328 of the Penal Code.

LAW OF COMBATING TRAFFICKING IN PERSONS NO. 28 OF 2012 IN IRAQ AND NO 6. OF 2018 IN THE KURDISTAN REGION

This specialized law, designed to combat Trafficking in Persons (TIP) in Iraq and the KRI, prohibits human trafficking in all forms, which is defined as an *"act of recruitment, transportation, transfer, housing, or receipt of persons through threat or use of force or other forms of coercion, kidnapping, fraud, deception, misuse of power, exchange of money, or privileges to an influential person in order to sell and exploit the trafficked individuals by means of prostitution, sexual abuse, unpaid labor, forced labor, enslavement, beggary, trading of human organs, medical experimentation, or by other means."* The law provides that if any form of human trafficking is committed against a minor, a woman, or a person with a disability, it will be considered an aggravating circumstance and warrant more severe punishment.

This law does not include specific provisions pertaining to online violence. However, the definitional scope of TIP is broad enough to include cases in which acts of TIP occur online or digital means are used in the course of committing such actions. This may include some forms of TFGBV and TF-CSEA, provided the definitional elements of TIP are met. For example, traffickers may begin by stalking and blackmailing women, gradually coercing or forcing them into prostitution or other forms of commercial sexual exploitation. In some instances, traffickers may exploit children for live-streamed sexual abuse, producing illegal content for financial gain. However, applicability of the law is limited to violations occurring within the context of trafficking, and not to instances of online violence, including acts of sexual abuse and exploitation against women and children, that occur outside of that context.

Furthermore, the response to recognized violations is not sufficient in practice. Implementation of the Law of Combating Trafficking in Persons across Iraq and the KRI is not unified nor consistent due to conflict with other penal codes, particularly the Iraqi Penal Code No. 111 of 1969, 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. The variable application of these laws can result in the prosecution of survivors and may deprive them of available protections. Additionally, conflict between applicable laws can result in confusion between the diverse institutions responsible for handling such crimes, including the Directorate of Combating Organized Crimes (DCOC) in the KRI and the Directorate of Combating Human Trafficking in Iraq, the Directorate of Combating Violence Against Women and Families (DCVAW), regular police, and specialized courts.[35] Additionally, the law does not address existing resource limitations among relevant institutions, such as deficits in capacity and technical expertise to investigate online forms of trafficking, including those falling under the definitions of TFGBV and TF-CSEA, or the lack of basic equipment to preserve, store, and analyze online data. The law also does not include procedures on the identification of these violations and the appropriate management of electronic data.

5.3.4. LAW ON PREVENTING MISUSE OF TELECOMMUNICATION DEVICES NO. 6 OF 2008 IN THE KURDISTAN REGION

In 2008, the Kurdistan Parliament 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. As a specialized law, its provisions take precedence over those stipulated within general laws, such as the Iraqi Penal Code No. 111 of 1969, when those provisions are in conflict. However, it is only applicable in the KRI.

This law was enacted in response to social, economic, and political developments driven by new and complex technologies, as well as the impact of those technologies on the lives of individuals, particularly children and youth.

35. If a parent arranges to sell a child into sexual slavery or use a child for begging, for instance, the case may fall at the intersection of both DCOC and DCVAW mandates.

LAW ON PREVENTING MISUSE OF TELECOMMUNICATION DEVICES NO. 6 OF 2008 IN THE KURDISTAN REGION

In its founding rationale, the law stresses that the Kurdistan Region strives to establish a healthy civil society in which individual rights and freedoms are protected. It also reiterates, in Article 1, the importance of the right to privacy, stating that: *"telephone calls, postal and electronic communications are private and inviolable."* It is well established that this law was intended to protect privacy by combating any misuse of communication tools and methods.

The law, which consists of 8 articles, identifies criminal behaviors that amount to online violence and then delineates punishments for such actions. It also establishes an accountability mechanism for communication companies with regard to the registration of communication devices and the provision of information to the competent judicial authorities, if requested.

In Articles 2 and 3, the law defines criminal conduct related to the misuse of communication devices under two main categories. Article 2 states that:

[...] any person who misuses a cell phone, any telecommunications device, the Internet or e-mail for the purpose of threatening, slandering (defamation), insulting or spreading fabricated news that provokes terror, leaking a conversation or a picture (animated and inanimate), spreading SMS contrary to public morals and ethics, taking photographs without permission, any action that undermines honor, inciting to commit crimes or immoral acts, publishing information relating to private or family life secrets of individuals obtained in any way, even if true, if their dissemination, diversion and distribution would offend or harm them, shall be detained for no less than six months and no more than five years and fined for no less than one million IQDs and no more than five million IQDs, or one of those punishments.

Article 3 stipulates that:

[...] anyone who intentionally uses and exploits a cell phone, any telecommunications device, the Internet or electronic mail to disturb others in cases other than those mentioned in Article 2 of this Law shall be liable to detention for a term of not less than three months and not more than one year and a fine of not less than seven hundred and fifty thousand dinars and not more than three million dinars.

Based on the provisions in Articles 2 and 3, the following criminal behaviors amount to online violence, if committed via a communication device, the internet, or other online systems:

- Threatening, slandering (defamation), and insulting;
- Spreading fabricated news that provokes terror;
- Leaking conversations (e.g. online calls) or animated and inanimate pictures;
- Spreading SMS with content that is contrary to public morals and ethics;
- Taking photographs of an individual without permission;
- Committing any action that undermines honor and brings shame;
- Inciting individuals to commit crimes or immoral acts;
- Publishing information relating to the personal or family life secrets of individuals, if such an act harms them;
- Disturbing others in any form.

Article 6 of the law introduces an accountability mechanism for telecommunication companies. First, it obligates telecommunication companies working in the KRI to register SIM cards and electronic communication devices in the name of the non-subscribing holder within six months from the date the law entered into effect. Accordingly, the concerned companies are required to cancel any SIM cards whose holders fail to register during that period. Second, the telecommunication companies must provide information on SIM cards and users when requested by the competent authorities. The law states that companies in violation of these obligations *"shall be liable to an amount of fine not less than 50 million IQDs and not more than 100 million IQDs."*

While the Law on Preventing Misuse of Telecommunication Devices No. 6 of 2008 does not explicitly address TFGBV or TF-CSEA, it still offers basic protections for survivors and those at risk. The broad array of offenses outlined in Articles 2 and 3 offers positive protections and mechanisms within the law's capacity to address a wide range of online violence manifestations, such as image-based abuse, hate speech, defamation, online stalking, sexual harassment, and more.

However, there are many forms of TFGBV and TF-CSEA that are not addressed by this law, and the offenses named within it are defined in broad and imprecise terms, leaving room for variable interpretations when applied on the ground by the judiciary. While this could be perceived as an advantage for survivors of online violence and those at risk, the major challenge with broad definitions of criminal acts is the confusion they may cause, affecting prospects for widespread and consistent public awareness. As a result, individuals who experience specific forms of online violence may not realize that such behaviors constitute recognized crimes and therefore may not pursue justice via the legal system, impeding their ability to access key rights

and protections. Importantly, this broad definitional approach also contradicts the recognized principles of the Iraqi criminal justice system, which require descriptions of criminal acts to be precise and clear to every lay person in order to facilitate the ability of the public to uphold the social contract through appropriate behavior.

Moreover, in the absence of definitional precision, the provisions in the law can be used by authorities to prosecute individuals who exercise freedom of expression and opinion online. Significantly, the main application of this law has not centered upon the prevention of online violence, inclusive of TFGBV and TF-CSEA, or the enactment of protective measures in response to them. While the law calls for the protection of individuals from online violence, in practice, it has been used to suppress free use of the internet and free speech, particularly as it concerns criticism of the government.[36] The broad provisions in the law have been leveraged to prosecute individuals who accuse government officials of failing to support the public interest, whether by posting comments on social media platforms and in chat groups, or by publishing articles online. The broad nature of the law also delegates significant discretionary power to the judiciary in terms of tailoring the law to the facts of a case and determining punishments for criminal behaviors. The scope of possible punishment ranges from detention of three months to five years, and/or a fine from one to five million IQDs. While criminal codes often grant some discretionary power to the judiciary to determine an appropriate punishment based on the circumstances of a particular violation, this law surpasses normative limits in the delegation of discretionary power. For instance, a person leaking a phone conversation could be punished with a term of detention of five years or something significantly more minimal, such as a fine of one million IQDs.

Notably, in its current form, the law does not mandate a specialized institution or unit to handle cases of online violence, nor prescribe how these cases should be managed by the relevant authorities. Unlike other specialized laws in the KRI – such as the Law of Combating Domestic Violence No. 8 of 2011, which mandates DCVAW to lead on efforts to prevent and respond to domestic violence – the Law on Preventing Misuse of Telecommunication Devices No. 6 of 2008 leaves the response to online violence in the hands of the general apparatus responsible for addressing all types of crime, comprising the regular police, investigative courts, and trial courts.

Another deficit in the law is that it does not introduce any special procedures or protections for victims of criminal offenses based on survivor centered and human rights-based approaches. In the absence of special procedures within the law, the general provisions of the Iraq Criminal Procedural Law No. 23 of 1971 apply. These procedures and safeguards are designed for the prosecution of offline violations and are not necessarily compatible with online violence, which occurs in the online or digital sphere. An effective response to online violence should include specific, survivor-centric procedures relevant to such violations, including the procurement of informed consent and the exercise of privacy and confidentiality in all circumstances, including when complaints are filed by survivors. From a technical perspective, the law should also adopt specific procedures on the search, seizure, confiscation, and preservation of online data and should introduce procedural safeguards, including judicial supervision, to govern the management of personal data. The law also does not delineate available protections for survivors of online violence in terms of short-term and long-term solutions. These protections might include ensuring the safety and security of survivors, as well as facilitating their access to basic services, particularly mental health, psychosocial support, and legal services.

Promoting the accountability of telecommunication companies is an essential preventive measure to combat online violence in the KRI and Iraq. However, while the law does address the issue of unregistered SIM cards and devices, these provisions have yet to be implemented. In the KRI, there is a significant number of unregistered and unknown SIM cards and devices on the market that can be freely purchased and used. Telecommunication companies within the KRI have not complied with the provisions of this law and have not been held accountable.

Finally, the law does not include necessary prevention measures that are supported by allocated resources. Examples of robust prevention measures might include raising the awareness of individuals (e.g. adolescents, parents, and caregivers) and communities; developing an online safety curriculum for public and private schools; establishing platforms to disseminate and serve as a repository for online safety instructions and other educational materials; strengthening institutional capacity via law enforcement and the judiciary; and moderating online content and developing standard operating procedures for online media. A comprehensive approach to combating online violence should be built into the existing legislative framework, requiring cross-sectoral collaboration across various government institutions.

36. Freedom of Expression in the Kurdistan Region of Iraq (UNAMI & OHCHR, 2021).

5.3.5. LAW OF COMBATING DOMESTIC VIOLENCE NO. 8 OF 2011 IN THE KURDISTAN REGION

While federal Iraq does not have a domestic violence law, the KRG enacted the Law of Combating Domestic Violence in 2011.

LAW OF COMBATING DOMESTIC VIOLENCE NO. 8 OF 2011 IN THE KURDISTAN REGION

This specialized law, applicable in the KRI, is designed to address domestic violence – or violence within the family – in all its physical, psychological, and sexual forms. The law does not specifically reference prevalent forms of online violence against women and children, such as TFGBV and TF-CSEA. However, in the absence of strong legislative frameworks to address online violence, some provisions of this law may potentially be applied to online violations, provided those violations fall within the definition of domestic violence. For example, if a husband blackmails his partner online, forcing her to stay in the marriage or carry out certain behaviours, or a family member exploits a child for sexual purposes through explicit images, live streaming, or online gaming, such scenarios may be addressed within the confines of this law. However, applicability is limited to violations occurring within the family, and is not sufficient to address online violence against women and children more broadly.

5.3.6. DRAFT LAW ON COMBATING CYBERCRIMES IN IRAQ

Long term efforts to regulate online crimes at the federal level have not yet resulted in the enactment of a specialized law. However, a draft Law on Combating Cybercrimes in Iraq was first introduced to the Iraqi Council of Representatives (COR) in 2011, and again in 2019. While the COR committees have continuously sought to legislate this draft since its creation, it has never passed due to its shortfalls, gaps, and potential to restrict freedom of expression.[37] The founding rationale and objectives of the draft centralize its aim to provide protection for the legal and legitimate use of computers, information networks, and data, and to establish a punitive system for perpetrators of cybercrimes in light of the emergence, growth, and ongoing development of technology and means of communication. While not specifically designed to address TFGBV and TF-CSEA, the draft law regulates all criminal behaviors that occur online via one of the means of communication. An analysis of the most recent version of this draft law, which was first circulated in 2022, is provided below, following the suggested structure of the draft itself.

Definitions

The draft law provides a list of 29 definitions, which includes mostly technology-related terms along with substantive and procedural criminal law terms. It defines computer, information, information technology, data, classified and unclassified government data, electronic data processing, website, password, subscriber, subscriber's information, service provider, electronic card, network, electronic and numeral signature, electronic means of communication, permission, and numeral evidence.

The draft defines cybercrime as an *"act committed using a computer, information network, or other information technology means, punishable according to the provisions of this law."* It defines eavesdropping as *"to look into or access data and information without permission"* and illegal access as *"unpermitted or illegal access to an information system, network, or computer."* It defines electronic blackmail as *"the operation of threat or terror to spread special information or data in exchange for money or doing work in favor of the perpetrator or causing physical or psychological damage to another person."*

The list of definitions is very long and confusing for a number of reasons. The majority of the definitions are not necessary, are redundant, or are already defined in another law, thus creating confusion for law enforcement and the judiciary, who will be responsible for applying this law in the future. For example, "government data" is defined as the types of data that are owned by the government, while "classified data" is defined as data that is classified by law. Such definitions do not add nor provide needed clarity with regard to the meaning and use of these terms. The draft law also defines "permission" in the context of service provision, when this term should be defined in other laws or regulations, such as the communication-related laws which regulate the permission of communication service providers. Moreover, the draft law defines electronic incitement to commit online violence; however, any incitement to commit a crime, whether online or offline, is already regulated by the provisions of criminal participation in the Penal Code and there is no need to repeat it in the law.

The number of definitions has also changed significantly from one version of the draft law to the next. For instance, the 2019 draft includes eighteen definitions, while the 2022 version includes twenty-nine. The process of developing this draft law over the course of many years may mean that new additions to the text have not been properly examined in context. Thorough revision is required to create a shorter list with precise definitions.

The draft law does not currently incorporate relevant provisions

37. New Attempts to Issue the Cybercrime Law in Iraq: alaraby.com.uk

from international conventions that regulate online crimes, in particular the Arab Countries Convention. Such conventions provide clear and necessary definitions of terms, including computer system, information technology and network, data, service provider, and subscriber's information.

Substantive Law

The draft law provides fourteen sections on different forms of cybercrime. While it does not explicitly reference TFGBV or TF-CSEA, a number of these provisions are relevant to online violence, including acts which fall within those categories. The following analysis highlights several offense categories from the draft law that are particularly relevant to TFGBV and TF-CSEA.

Offenses of Illicit Access and Illicit Interception:

In this category, the main criminal activities include intentionally entering or remaining on a website, network, or computer without permission or right, and eavesdropping and intercepting data or information in networks or communication devices without permission or right. Multiple forms of TFGBV, such as hacking and cyberstalking, fall within this category. The punishment of these behaviors increases if the act leads to modification, distortion, removal, or destruction of data, electronic instruments, and networks, or if conducted on the classified information of the government, and varies based on the severity of the offense. It generally includes detention or imprisonment for one year to fifteen years, a fine ranging in amount from five to thirty five million IQDs at minimum, or one of those punishments.

Offense of Misuse of Technology Information Means:

In Article 7, the draft law criminalizes the production, sale, purchase, import, distribution, or provision of any tools or programs, passwords, or access codes designed for the purpose of committing the offenses stipulated in the draft. These offenses may be directly linked to acts of both TFGBV and TF-CSEA. For instance, a person may create a serial number to hack an application or enter someone's account to steal personal information or photos, or a person may produce an application specifically for editing photos and videos in a degrading way. Punishment for such offenses includes detention from 24 hours to five years and a fine not less than ten million IQDs.

Offenses Related to Online Pornography:

To strengthen protective measures against sexual exploitation, Article 11 of the draft law criminalizes three categories of activity under offenses related to online pornography. First, it criminalizes acts of production, display, distribution, provision, publication, purchase, sale, and import of pornographic material or indecent materials through information technology for commercial purposes. Punishment for these actions is detention for no more than four years and a fine no less than twenty-five million IQDs. Second, it prohibits acts of legitimation, incitement, and publication of prostitution and sexual exploitation through information technology. The punishment for these actions is imprisonment for no less than six years and a fine no less than twenty million IQDs. Third, it names acts of publishing a shameful picture of a minor (or a person appearing to be a minor) engaged in sexually explicit conduct, as well as acts of publication, production, distribution, purchase and sale, or importation of a shameful picture of a minor through information technology. Child pornography, the term used in this draft to describe such violations, is a severe form of child exploitation and abuse. The punishment for this last category is imprisonment for no less than ten years and a fine no less than fifty million IQDs.

Provisions that criminalize the sexual exploitation of children, including child pornography, are contained within a number of domestic laws.[38] However, the ever-increasing use of the internet as the primary instrument for such activities is not addressed. Through the provisions of Article 11, this draft law widely criminalizes child pornography as a form of online violence committed against children, providing a strong foundation for combating TF-CSEA.

Offenses of Assault on Personal Rights:

Article 12 of the draft law criminalizes certain acts that constitute an assault on the personal rights of individuals, including:

- The act of spying, upsetting, or stalking users of computers and computer networks without right, or publishing the personal information of an individual without permission.
- The direct or indirect use of someone else's computer device without permission or right.
- The use of a computer or information network to defame or insult another individual through the imputation of pictures, voices, indications, and anything else with defamatory or insulting content to another individual.
- The act of offending or insulting someone, or sharing and publishing information in that regard via technological means.
- The act of sending or transferring a message, an event or incident, or an electronic document, with the knowledge of its threatening and upsetting content, via a computer device or information networks.
- The act of threatening and blackmailing another person via a computer device or information network in order to commit a crime against him/her or his/her property.
- The act of publishing inflammatory sectarian, ethnic, or religious content via technological means.

A number of the aforementioned acts could constitute various forms of online violence that fall under the definition of TFGBV, including image-based abuse, blackmailing, harassment, hate speech, defamation, and more. Punishment for these offenses

38. Including the Iraqi Penal Code No. 111 of 1969, the Law of Combating Prostitution and Homosexuality No. 8 of 1988 (Iraq) and the Law of Combating Prostitution No. 8 of 1988 (KRI), and the Law of Combating Trafficking in Persons No. 28 of 2012 (Iraq) and No 6. of 2018 (KRI).

includes detention or imprisonment for 24 hours to seven years and a fine no less than five million IQDs, or either of those punishments.

Organized Cybercrimes:

Article 10 of the draft law criminalizes the creation of a website or network for the purpose of human trafficking and/or drug trafficking. It also criminalizes the creation of a website or network to facilitate, assist, or promote human and/or drug trafficking, including for the purpose of arranging contracts or negotiations to make deals related to trafficking. The punishment for these acts is imprisonment for 20 years and a fine in the amount of 35 million IQDs. By explicitly criminalizing the digital dimensions of trafficking and acknowledging that such acts can be committed or facilitated via the internet and communication means, the draft law ensures that trafficking as a form of TFGBV and TF-CSEA can be addressed.

The remaining cybercrime categories covered in the draft law include: offenses against state security; assault against electronic documents and signatures; online forgery and inception; offenses related to online payments; offenses related to intellectual property; offenses related to providing information; and offenses related to service providers.

In terms of its substantive rules, the draft law identifies several general categories of offenses that connect to online violence. However, many of these categories are defined in vague and broad terms, which increases the risk that they may be interpreted in a manner that restricts fundamental rights and freedoms. For example, provisions related to national security and terrorism offenses could potentially grant authorities expansive powers that could be used to monitor the online activities of citizens and prosecute individuals for expressing dissenting political views online – undermining the rights to freedom of expression and access to a free internet. Additionally, some of the punishments identified for specific offenses are extremely severe, rather than proportional and necessary.[39] The draft law also delegates significant discretionary power to the judiciary to tailor the rules to the facts of a case and determine punishments accordingly. These characteristics increase the potential for abuse.

Procedural Law

The draft law provides some procedures and measures to facilitate the collection of evidence and investigation of cybercrimes in Article 17. These provisions are designed to accommodate the electronic and fast-changing nature of cybercrime. However, they are not designed to respond to online violence, specifically, and lack survivor-centered approaches and safeguards.

With regard to the expedited preservation of data, the draft authorizes a specialized judge to order any entity in their territory to submit specified computer data, within that entity's possession or control, for storage in a computer system or a computer-data storage medium, where there are grounds to believe that data is particularly vulnerable to loss or modification.

The draft provides that the competent investigation or trial court may order a service provider to submit subscriber information if such information contributes to crime detection. Such orders can also be used to authorize the competent court to monitor computer systems and networks if there is a suspicion of cybercrime, with the condition that the possessor of such a system or network must be informed about the measures and duration of monitoring. This should help to ensure that measures taken represent a proportional response to existing threats and do not violate the rights of others. Additionally, the competent court can order seizure of a computer or part of it, transfer of these assets to the investigation site, and replication of the data for investigation purposes.

Article 18 of the draft law provides that a specialized center for cybercrimes and electronic evidence will be established, which will be regulated through a bylaw. While the draft law establishes a specialized center to handle cybercrime in general, it lacks any information on the center's structure, mandate, and authorities, which ought to be regulated within the law and not determined by executive powers. Given the center's extensive authority to access computer systems and networks, this should be closely regulated. Moreover, the draft does not regulate the relationship between the center and the judiciary, nor stipulate whether the center is an executive agency or under the supervision of the judiciary. The draft law establishes some special criminal procedures for handling electronic data and investigating cybercrimes. The recommended safeguards guarantee that there will be effective judicial supervision of – and justified grounds for – these interventions to avoid violating the rights of third parties.

Importantly, however, the draft law lacks survivor-centric provisions to address sensitive matters like TFGBV and TF-CSEA. While the law addresses the criminal aspects of online abuse to some extent, it fails to include essential measures for the protection of those affected, particularly women and children. It does not stipulate the minimum standards for victim assistance – such as access to legal aid, psychological support, or safety measures for those affected by online violence – nor does it establish institutions with the necessary expertise to assess the physical and psychological well-being of survivors and provide the required support services. It also fails to ensure that victims can access these services without being required to file a formal complaint, which may discourage some individuals, particularly women and children, from seeking the help they need in the aftermath of abuse. It also lacks appropriate procedural safeguards to ensure that survivor consent and confidentiality is preserved throughout the response process. These oversights undermine the draft law's potential to fully address the needs of survivors and ensure their rights and well-being are protected.

39. For instance, illegal access to a website is punishable by detention for up to five years and a fine of at least five million IQDs.

5.4. REGIONAL LEGISLATIVE RESPONSES TO ONLINE VIOLENCE

Various legislative approaches have been adopted across the Middle East and North Africa (MENA) region to address the prevalent threat of online violence. Some nations have amended their existing penal codes and laws to cover both online and offline forms of violence. Others, such as Kuwait, Jordan, and the United Arab Emirates, have introduced specific laws to combat cybercrime. However, these laws are not specifically focused on online violence, including against women and children, and often fall short in addressing all aspects of an effective response.[40] Additionally, many frameworks within the MENA region have been criticized for facilitating suppression of digital rights, underscoring the critical need for balance when regulating online behaviors to combat harm while protecting fundamental freedoms.[41]

The neighboring country of Kuwait, which has a similar culture and criminal justice system, has also experienced the compounding effects of vulnerability to violence and the widespread use of advanced technologies. As a comparative exercise, this legislative analysis evaluates the approach that Kuwait has taken to combating cybercrimes, including via the enactment of legal provisions and protections related to TFGBV and TF-CSEA, in order to highlight the shortfalls of the framework and integrate best practices and lessons learned in the concluding recommendations.

Prior to legislating Law No. 63 of 2015 on Combating Information Technology Crimes, the Government of Kuwait applied the general provisions of Penal Code No. 16 of 1960 to offenses in the digital dimension. However, the general provisions within the Penal Code of Kuwait are not sufficient to combat cybercrimes committed with advanced technological means; protect the freedoms, honor, and reputation of individuals; or prevent assaults on public and private trusts. These shortcomings can be attributed to the fact that the Penal Code uses broad terms and definitions which introduce a significant possibility of misuse in light of technological advancements. Like Iraq, Kuwait ratified the Arab Countries Convention and, following that ratification, enacted Law No. 63 of 2015 on Combating Information Technology Crimes.

KUWAIT LAW ON COMBATING INFORMATION TECHNOLOGY CRIMES NO. 63 OF 2015

The law is composed of two sections. The first section, in Article 1, lists the definitions of relevant information technology terms, including electronic data, computer system, networking system, information system, website, cybercrime, illegal inception, electronic signature, information tracking and electronic fraud.

The second section, in Articles 2- 15, outlines provisions on various cybercrimes, including:

- Illegal interception of a computer or its system, or an electronic data processing system, or an automated or information network. This includes criminal acts such as illegal access and the cancellation, deletion, destruction, disclosure, alteration, or re-publication of data. The crimes are aggravated if the assault is conducted on the private information and personal data of an individual. The law also considers it an aggravating circumstance if the perpetrator is a government employee who commits such acts during work or to fulfill official duties.
- Illegal interception of classified information belonging to the government, including attacks on banking systems and their data.
- Forging or damaging a document, computer system, or electronic system via fabrication, alteration, modification, or by any other means.
- Use of an information network or any means of information technology to threaten or blackmail a natural or legal person in order to compel her/him to do or refrain from doing something. It is an aggravating circumstance if the threat is to commit a felony against the person or his/her dignity or honor, prestige, or reputation.
- Intentional eavesdropping on, capturing, or intercepting a transmission by an information network or other communication means. It is considered an aggravating circumstance if the content of the transmission is disclosed.

40. Violence against women in the online space (UN Women, 2021).

41. NB: In 2023, Jordan enacted Cybercrime Law No. 17 with the intention of curbing online violence and combating cybercrime. However, the law has been misused to severely restrict freedom of expression and to prosecute journalists, media practitioners, and others who have criticized government policies, resulting in calls for it to be repealed or amended. The United Arab Emirates enacted an initial Combating Cybercrime Law No. 5 of 2012, which was later amended to address technological advancements and the widespread use of the internet, leading to the introduction of a new Cybercrime Law No. 34 of 2021. Despite being paired with a Data Protection Law No. 45 of 2021 to better regulate and protect digital activities and personal data, this law also features provisions that criminalize online speech and content under vague and imprecise terms, increasing the risk of misuse to silence dissent or curb freedom of expression.

- Creation or use of websites, or publication of information via technological means, to promote human trafficking or illegal drugs.
- Creation or use of websites, or publication of information via technological means, to promote terrorism by an organization or an individual.

It is considered an aggravating circumstance if the victim of any acts listed above is a minor, legally incompetent, or has been exploited in any form.

Law No. 63 of 2015 on Combating Information Technology Crimes generally regulates cybercrime in all forms. This framework does not include explicit provisions on TFGBV or TF-CSEA. However, it does criminalize certain online behaviors that may amount to or be involved in the commission of these crimes, including hacking, illegal access to personal or private information on computers and systems, threatening, blackmailing, exploitation of minors, trafficking activities, and so forth. For a more robust response to online violence against women and children, this law can be complemented by the application of other relevant protective frameworks, such as Kuwait's Domestic Violence Law No. 16 of 2020 and its Child Rights Law No. 21 of 2015, the latter of which specifically prohibits the use of children for sexual purposes through modern communication tools and the importation, exportation, production, preparation, and distribution of any pornographic material involving children or related to child sexual exploitation – key forms of TF-CSEA.

Kuwait's Law No. 63 of 2015 is more precise in its terminology than existing Iraqi laws and Iraq's draft Law on Combating Cybercrimes. The punishments stipulated in Kuwait's law are also less severe than in Iraq's draft law, and the judiciary is not given unregulated discretion to prosecute and punish within a dramatic range of options. For example, the punishment for illegal interception in Iraq's draft Law on Combating Cybercrimes is a term of detention or imprisonment not less than a year (with a maximum term not stipulated) and a fine not less than 5 million IQDs, or around $3,820 USD (with a maximum amount not stipulated), or one of these punishments. In Kuwait's Law No. 63 of 2015, the punishment for the same behavior is a term of detention not more than six months (the minimum can be 24 hours) and a fine not less than 500 Kuwaiti Dinars and not more than 1,000 Kuwaiti Dinars (a range between $1,637 to $3,274 USD).[42]

The law importantly mandates the Department of Electronic and Cyber Crime within the Ministry of Interior to combat electronic and cybercrimes and work closely with the Anti Human Trafficking Department. This department, which has established both online and in-person mechanisms to facilitate reporting of electronic and cybercrime incidents, is mandated to handle interrogations and investigation with high consideration for procedural safeguarding. The department also focuses on building relevant expertise, allocating technology-related resources, and conducting awareness campaigns,[43] particularly targeting children.

However, similar to Iraq's draft Law on Combating Cybercrimes, Kuwait's Law No. 63 of 2015 lacks survivor-centered provisions to address critical needs and secure important protections for survivors of online violence. Moreover, both the Iraqi and Kuwaiti frameworks fail to include provisions on accountability mechanisms for telecommunication companies to regulate the means of communication to effectively combat online violence and promote safe access to the internet. Kuwait's Law No. 63 of 2015 also fails to integrate appropriate safeguarding measures with regard to the collection and expedited preservation of data to avoid intrusion on fundamental rights and freedoms.

6. INSTITUTIONS IN IRAQ AND THE KURDISTAN REGION

In Iraq and the KRI, online violence in general – including TFGBV and TF-CSEA – is not regulated by a clear, cohesive, and comprehensive legislative framework. Therefore, no institutions with an explicit legal mandate to combat these crimes exist. As a number of general and specialized laws criminalize certain behaviors or acts amounting to TFGBV and TF-CSEA, the institution responsible for addressing such acts may vary based on the specific framework applied by the judiciary.[44] In practice, there are a few relevant institutions working to address online violence in Iraq and the KRI. However, these institutions are typically not specialized in TFGBV or TF-CSEA, nor clearly mandated by law to combat these crimes. This section provides a brief analysis on some sector-specific institutions involved in shaping the response to cybercrime and online violence, and identifies the constraints these institutions face in the absence of a comprehensive legal framework.

42. According to the World Bank data, Iraq 's GDP per capita is $6,074 while Kuwait's is $32,214.

43. For more information, see the State of Kuwait Ministry of Interior Department of Electronic and Cyber Crime website.

44. For example, if a violation is categorized or described by a judge as falling under the Iraqi Penal Code No. 111 of 1969 or the Law on Preventing Misuse of Telecommunication Devices No. 6 of 2008 (KRI), in which no other responsible entity is identified, the regular police have the authority to handle the case. However, if the violation falls under the Law of Combating Trafficking No. 28 of 2012 (Iraq) and No 6. of 2018 (KRI), or the Law of Combating Domestic Violence No. 8 of 2011 (KRI), the respective entities responsible for combating human trafficking or domestic violence have the mandate to respond. On the procedural side, responses by any of the above institutions are generally governed by the provisions of the Iraqi Criminal Procedure Law No. 23 of 1971.

6.1. COMMUNICATIONS AND MEDIA COMMISSION IN IRAQ

The Communications and Media Commission (CMC) is an independent federal institution concerned with regulating media and communications in Iraq under Executive Order 65 of 2004 and the Iraqi Constitution (Article 103/A). Its mission is to organize and develop the media and communications sector in Iraq, in line with modern international standards. The GOI assumes responsibility for developing strategic policies in regard to communications, while the CMC is responsible for their implementation. The CMC exercises authority in regard to:

- Regulating broadcasting, telecommunications networks, and other services – including licensing, pricing, and internal connectivity – and defining fundamental conditions for providing public services.
- Planning, coordinating, distributing, and determining the use of broadcast frequencies.
- Organizing media designs and developing press mechanisms.
- Establishing, developing, and strengthening election media regulations.
- Supporting and encouraging media-related vocational capacity building and the adoption of professional behavior directives in the media.
- Developing and publishing communication and media policies, and proposing laws to the government and concerned authorities in this regard.

The CMC has considerable authority to prevent and respond to online violence, including by strengthening the accountability of media and telecommunication companies via regulations and monitoring the implementation of professional and ethical codes. However, the CMC has faced significant challenges in terms of balancing between protected interests in the fulfillment of its mandate. In March 2023, for example, a leaked copy of the CMC's draft Regulation No. 1 of 2023 for Digital Content in Iraq was heavily criticized for restricting freedom of expression and other related freedoms stipulated in the Iraqi Constitution, as well as expanding the authority of the CMC, at the expense of the legislature, by defining wrongful acts and determining punishments.[45] Additionally, while the CMC is a federal agency with authority nationwide, it has also faced significant challenges in ensuring compliance with relevant decisions and directives.[46] To support consistent and widespread enforcement, the CMC should work to enhance collaboration among all stakeholders and strengthen cooperation between the national and regional governments.

6.2. MINISTRY OF INTERIOR IN IRAQ AND THE KURDISTAN REGION

The Ministry of Interior (MOI) in both Iraq and the KRI lacks a specific entity legally mandated to combat and respond to online violence, inclusive of TFGBV and TF-CSEA. In the absence of an appropriately mandated institution, the regular police and the investigative courts are typically responsible for interrogation and investigation in TFGBV and TF-CSEA cases. However, given the complex nature of these crimes, particularly in terms of the intangible evidence and rapidly changing circumstances within the online sphere, it is imperative that the government allocates appropriate human and technical resources to ensure that the institutions combating these crimes have the requisite capacity and expertise to do so effectively. Identifying and resourcing actors who are well-placed to lead on the response to online violence is key to deterring crimes, providing a safe and secure digital environment, and protecting individual rights and freedoms without unlawful intrusion.

The establishment of specialized, legally-mandated directorates within MOI has proven to be a promising approach to enhancing governmental capacity to address particularly complex or uniquely patterned violences. At the regional level in the KRI, for example, the establishment of DCOC and DCVAW has strengthened institutional responses to combating human trafficking and domestic violence, respectively. These specialized directorates have been supported and capacitated by both government and NGOs to carry out their duties on the basis of recognized national and international standards.

In contrast to these legally-mandated directorates, other entities established within MOI via executive regulations or internal instructions – including those instated with the explicit aim of combating cybercrime, such as the federal Combating Cybercrime Unit – may have more restrictive mandates, limited geographic coverage, fewer available service types and modalities, and fewer technical and material resources, impeding their ability to leverage effective responses to specific protection concerns. This analysis will provide examples of both approaches.

45. Profile: Communications and Media Commission (The Washington Institute, 2023).
46. On March 13, 2024, the Federal Supreme Court issued a decision (No. 325 and 331/2023) mandating the Communications and Media Commission (CMC) and Ministry of Communications to take action to block all websites that promote pornography, presumably inclusive of child sexual abuse materials (CSAM), in partnership with tech companies and ISPs. However, several companies have yet to comply.

6.2.1. DIRECTORATE OF COMBATING ORGANIZED CRIMES IN THE KURDISTAN REGION AND DIRECTORATE OF COMBATING HUMAN TRAFFICKING IN IRAQ

In the KRI, DCOC is mandated by the Law of Combating Trafficking No 6. of 2018 and its associated regulations to respond to trafficking in persons in all forms. At the federal level, while a Committee for Combating Human Trafficking was established by the Law of Combating Trafficking No. 28 of 2012 to develop plans and programs, make recommendations and monitor implementation, report on progress in reducing human trafficking, and manage other assorted responsibilities, the Committee does not have the authority or legal mandate to investigate trafficking cases. In the absence of such a mandate, the response to trafficking cases is either managed by the Directorate of Combating Human Trafficking, established under MOI, or by the regular police in governorates where those units are not available.

Some recognized forms of online violence, such as those related to sexual exploitation and abuse, may be considered a form of trafficking and fall under the mandate of such entities if the definitional elements of TIP are met.[47] In addressing online violence within the context of TIP, however, the respective institutions in Iraq and the KRI face many legal and practical obstacles which must be addressed. Applicable laws should clearly cover online violence, mandate the appropriate institutions to work on all aspects of response, and ensure that those institutions are provided with the necessary human resources and expertise to handle such cases effectively. These frameworks should also integrate special procedures for detection, investigation, and management of electronic evidence. Addressing online violence in the context of human trafficking also requires close collaboration between regional and federal institutions and the judiciary, other law enforcement units, telecommunication companies, and NGOs, as well as effective coordination of investigations and prosecutions across countries and with the International Criminal Police Organization (INTERPOL).

6.2.2. DIRECTORATE OF COMBATING VIOLENCE AGAINST WOMEN AND FAMILIES IN THE KURDISTAN REGION AND DIRECTORATE OF PROTECTION OF WOMEN AND CHILDREN IN IRAQ

In the KRI, DCVAW is mandated to combat domestic violence under the Law of Combating Domestic Violence No. 8 of 2011. This directorate is responsible for investigating cases and providing assistance and protection to survivors. Its remit, however, only pertains to crimes perpetrated by family members (i.e. those with kinship to the fourth degree through blood or marriage, or those who are considered family by law). As a result, violence against women and children only falls under the mandate of DCVAW in certain circumstances, when such offenses occur within the family.

As a specialized unit, DCVAW may be well-positioned to manage cases of online violence. For over a decade, DCVAW has played a prominent law enforcement role in responding to cases of violence against women and children, and has led investigations and filed criminal cases on behalf of survivors. DCVAW employs diverse staff – including government officials, police, social workers, and lawyers, many of whom have received specialized training and capacity building on combating violence against women and children, as well as on survivor-centered and human rights-based approaches – and has reinforced its accessibility through the establishment of a hotline and active public engagement in awareness raising campaigns. Additionally, DCVAW carries out its activities under the supervision of the public prosecutor and the judiciary, which could help to guarantee greater protection of individual rights, such as freedom of expression and free use of the internet, in the process of combating online violence.

Notably, DCVAW has recently expanded its focus, in response to need, and begun absorbing online violence cases. While this is a promising development and DCVAW is well-situated to respond, it does not have an explicit legal mandate to respond to TFGBV or TF-CSEA, nor to any acts of violence occurring outside the family. DCVAW would also need to build additional skills, capacity, and expertise on technology-enabled offenses and investigation to complement its existing foundation in addressing offline forms of violence, and would need to strengthen collaboration and coordination across sectors to support a comprehensive response. Therefore, to be effective in addressing cybercrime, DCVAW's mandate would need to be expanded and additional support from the KRG would be required in terms of adequate human and financial resources, technical assistance, and authority to convene relevant actors.

At the federal level, MOI established the Directorate of Protection of Women and Children in 2009, which has 16 offices in major cities across Iraq and is responsible for receiving complaints and providing information to women and child survivors of domestic violence. However, in the absence of federal legislation on domestic violence, this department lacks a legal mandate to investigate these crimes. It also lacks adequate resources and technical capacity to combat violence outside the family, inclusive of online violence.

47. In other contexts, a specialized unit with a specific mandate to respond to specific forms of online sexual exploitation and abuse, such as TF-CSEA, is among the most prominent means of combating particular violations. For example, the government of Jordan has made rapid progress in responding to TF-CSEA. It established the Online Child Sexual Exploitation Prevention Unit in 2016 under the Juvenile and Family Protection Department to investigate TF-CSEA, in collaboration with the Anti Cybercrime Unit and Anti Trafficking Unit. The Unit also cooperates with INTERPOL to track abusers.

6.3. MINISTRY OF LABOR AND SOCIAL AFFAIRS IN IRAQ AND THE KURDISTAN REGION

The Ministry of Labor and Social Affairs (MOLSA) in both Iraq and the KRI is mandated to address social issues, which includes obligations to provide services to vulnerable groups – such as women, children, and the elderly – and develop policies and strategies to strengthen protections and care for those groups. Even in the absence of comprehensive legislation, women and children facing all forms of violence, whether offline or online, may be able to access essential support under applicable policies.

However, many of the key response entities that fall under the auspices of MOLSA face challenges in effectively managing cases of online violence, including TFGBV and TF-CSEA, due to deficits in requisite technical and technological expertise, shortage of human and financial resources, and restricted geographical coverage. Despite these limitations, MOLSA can play a significant role in several aspects of the broader response to online violence, including advocacy for needed legislative reforms, policy development, implementation of awareness campaigns, and strengthened collaboration with relevant law enforcement agencies and the judiciary to facilitate the delivery of coordinated, end-to-end support for those affected by online violence.

6.4. NATIONAL SECURITY AGENCIES IN IRAQ AND THE KURDISTAN REGION

At the federal level, in collaboration with other relevant agencies, the Iraqi National Security Agency is tasked with protecting the safety and security of the state and the community. The agency operates a helpline to receive complaints related to drugs, terrorism, and online harassment. However, this unit, which is predominantly focused on intelligence, is small, has limited geographic coverage, does not advertise the availability of in-person support, and is not sufficiently resourced to leverage a comprehensive response to TFGBV and TF-CSEA across Iraq.

The security agency in the KRI, Asayish, has dedicated units for ombating cybercrimes in two governorates. The Sulaimani General Asayish and Erbil General Asayish established cybercrime units in their respective governorate centers and, in 2023, published 24/7 helplines to facilitate reporting and subsequent investigation of online incidents under the supervision of a competent judge. However, the mandate of these units is based on internal instructions by the Asayish, rather than by law, and is not accessible to the public. Additionally, these units have limited geographic coverage and may not have equitable and sufficient resources, equipment, and technical capacity to address TFGBV and TF-CSEA across their operational locations.

7. KEY RECOMMENDATIONS AND PRIORITIES FOR LEGISLATION TO ADDRESS ONLINE VIOLENCE

This analysis concludes with key recommendations and priorities to inform the development of legislation to address online violence in Iraq and the Kurdistan Region. While action can and must be taken to strengthen leadership, improve coordination, and build expertise even in the absence of law, legislation is a critical strategy in the fight against online violence, as it provides the foundation for all aspects of an effective response. Therefore, to combat the growing threat represented by new and emerging forms of criminal activity in the digital dimension, including acts of TFGBV and TF-CSEA, the governments of Iraq and the Kurdistan Region should enact new laws or amend existing laws to address the deficits identified in this analysis, fully incorporating the international instruments ratified by Iraq and drawing upon global standards that are compatible with the local context.

A robust legislative response to online violence should, at a minimum:

- **Include Necessary Safeguards.** Recognizing that frameworks which criminalize behaviors in the digital environment are uniquely vulnerable to misapplication and abuse, and also recognizing that efforts to combat criminal activity can, if mismanaged, amplify risks for survivors, the law should provide necessary safeguards to govern all aspects of the response to online violence.
    - Explicitly recognize applicable rights and freedoms in the digital dimension, such as the right to privacy and protection of personal data, as well as the freedoms of opinion and expression, of press and media, and so forth.

- Include substantive and procedural safeguards[48] – informed by human rights standards and the core principles of legality, necessity, and proportionality – to protect those rights and freedoms and mitigate the risk of abuse in the application of the law.
- Integrate survivor-centered and rights-based approaches – including robust informed consent, confidentiality, and safeguarding protocols – throughout all processes[49] to ensure that the dignity, well-being, and wishes of survivors remain the basis for any action.

- **Establish a Comprehensive Approach.** To build a cohesive, integrated end-to-end response to online violence, the law should establish a comprehensive approach that includes measures for prevention, protection, prosecution, and reparation.
  - Precisely define the various criminal behaviors that constitute online violence, including acts falling within the categories of TFGBV and TF-CSEA, and determine clear and appropriate punishments for each criminal behavior.
  - Introduce new criminal procedures for the detection, investigation, and prosecution of online violence and technology-enabled offenses, including through the expedited preservation and management of electronic evidence and data.
  - Stipulate the remedies, protections, and services to which survivors of online violence are entitled, such as access to physical protection or shelter care, information, legal counseling, medical assistance, mental health and psychosocial support, and compensation.
  - Establish clear reporting mechanisms, such as a dedicated portal or hotline, with safe identification and referral pathways to connect survivors to available services and support.
  - Include measures to prevent online violence, such as national education programs and public campaigns to raise awareness of online violence, identify common risks and dangers, build digital literacy, promote online safety practices, and provide information on how to seek assistance.
  - Delineate regulatory obligations for electronic service providers and technology companies – such as registering devices, enforcing age restrictions on devices and platforms, providing safety tools, and enacting content moderation protocols and take down procedures – and create accountability mechanisms to ensure compliance.

- **Build an Institutional Framework.** To operationalize the response to online violence, the law should provide a clear institutional framework, with mandated leadership and mechanisms to support multi-layered interventions and coordinated action across relevant stakeholders and sectors, for a strong "whole systems" approach.
  - Establish a government-led, multi-stakeholder, cross-sectoral body to lead and coordinate the overall response to online violence. This body should ideally include relevant actors with a key role in addressing online violence – such as representatives from the regional or federal Ministries of Interior, Justice, Labor and Social Affairs, Health, Education, and Communications; the technology industry; and civil society, among others – and have the requisite authority to convene the same.
  - Designate a dedicated law enforcement agency or unit to combat online violence offenses, empowered by an explicit legal mandate. This agency or unit should possess the required specialist knowledge and technical tools to lead, support, and coordinate complex and sensitive investigations, as well as the capacity to coordinate with relevant international counterparts on transnational crimes.
  - Identify all other relevant agencies involved in the response to online violence, and clearly define their respective roles and responsibilities to address gaps, mitigate the risk of duplication, and promote effective inter-agency cooperation and coordinated action.
  - Incorporate provisions to support the harmonization or development of relevant policies within the proposed legal framework, such as national action plans and strategies, to synergize approaches and build a whole systems approach to combating online violence.

48. Such measures should ensure that any restrictions on fundamental freedoms are narrowly defined; criminal behaviors are precisely specified; penalties are proportional and necessary; access to evidentiary data is reasonable, for a specific purpose, and subject to rule of law safeguards to avoid arbitrary interference; investigation processes include independent supervision or oversight; powers granted to designated authorities are appropriately regulated to avoid overreach and ensure impartial access to justice and due process; and so forth.
49. For more information on how these principles should be specifically addressed throughout all processes, including the collection of evidence and evidentiary rules, legal procedures, and the rights of survivors during legal proceedings, please see: Handbook for Legislation on Violence Against Women (UN Women, 2012).

- **Design for Impact.** To ensure the efficacy of the response to online violence, the law should include measures to support implementation, monitor and evaluate progress, and facilitate adaptation as needed.
    - Provide a specifically allocated, adequate budget to support implementation, and ensure that all mandated institutions are properly resourced to deliver on their respective legal obligations.
    - Integrate measures to build the expertise of key agencies across the response architecture – including law enforcement, judiciary, and the social services workforce – through systematic training programs and technical assistance, to ensure they are equipped to implement.
    - Create a system or mechanism for safely gathering, storing, and managing routine statistical data on online violence to track progress, report against measurable outcomes and indicators, and support evidence-based adjustments to strengthen implementation and improve the collective response.
    - Establish formal monitoring procedures, such as via a review process or committee, to periodically evaluate the efficacy of the framework, advise on the need for dynamic adaptations to keep pace with technological advancements and facilitate application to emerging forms of criminal activity, and foster accountability.


SEED