Digital Violence Against Women in Lebanon: Legal and Institutional Context

March
2024

Roula Zayat
Judge Anouar Mnasri

IDRC · CRDI
Canada

secdev.foundation

Acknowledgments

Research team

Roula Zayat (lead researcher) is Executive Director of the Arab Center for the Development of the Rule of Law and Integrity (ACRLI)–Lebanon. She is a legal researcher with over 10 years of experience promoting the rule of law and good governance. She has extensive experience in legal research and analysis as well as in designing and developing projects relating to the rule of law and human rights, and she has served as a consultant for a variety of international organizations.

Judge Anouar Mnasri (legal expert) is chief of the primary court at Tunisia's Administrative Court. She is also a founding member of the Tala Al-Mutadamina Association and the Tunisian Women Voters' League. She conducts legal research, particularly on civil space, women's access to justice, and gender-sensitive approaches to public policies. She also contributes to election observation reports from a gender perspective.

Editorial team

Dr. Nadia Al-Sakkaf (editor) is a scholar who focuses on political affairs and democratic processes in the Middle East. She is a former Editor-in-Chief for the Yemen Times, and Yemen's first-ever female Minister of Information.

Dr. Raed M. Sharif (editor) is Senior Regional Programme Manager for the MENA region at The SecDev Foundation. He is a digital rights expert focussing on digital violence against women in the Arab world.

Dr. Ahlam Mohammed (translation/copyediting) is a linguistics expert, MENA researcher, and author of several book chapters and peer-reviewed articles.

Additional credits

We also gratefully acknowledge the assistance of many additional contributors, including Dr. Fadia Kiwan, MP Cynthia Zarazir, activist Josephine Zogheib, Ms. Asmaa Hamada, activist Hayat Murshad, Mr. Charbel Al-Qarih, Mr. Charbel Shabir, Ms. Jan Akl, Ala Elfellah, Osama Moussa, Jesus Rivera and John Hall.

This study was originally written in Arabic.
You can find the original version here.

The Arab Centre for the Development of the Rule of Law and Integrity

This prominent Arab Regional NGO was founded in 2003 by a group of legal professionals from Lebanon and other Arab countries to advance the principles of rule of law, justice, and integrity across the Arab region. ACRLI's work helps strengthen public and private institutions, foster a culture of legality, and empower citizens to protect their rights. The center's initiatives have a direct impact on Arab governance and legal systems, promoting stability, justice, and long-term development.

The SecDev Foundation

The SecDev Foundation's Salama@ team supported this research as part of a series of 20+ studies on the psychosocial and legal dimensions of digital violence agaist women across the MENA region. Responsibility for any views expressed in this study rests with the research and editorial teams. Since 2011, this Canada-based NGO has worked globally to promote digital resilience among vulnerable populations—especially women, youth and at-risk civil society organizations.

International Development Research Centre

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada. Views expressed herein do not necessarily represent those of IDRC or its Board of Governors. IDRC invests in high-quality research in developing countries, shares knowledge with researchers and policymakers for greater uptake and use, and mobilizes global alliances to build a more sustainable and inclusive world.

Intellectual property

Abstract

Digital violence against women is a growing challenge in light of rapid technological advancement. This includes digital harassment, online threats, and privacy violations, with negative impacts on victims. International efforts have been made to address this, with some countries enhancing legal protection and punishment for perpetrators. Lebanon has enacted laws and adapted existing ones to address digital violence, but cases continue to rise, especially affecting underage girls. This study analyzes Lebanon's response to digital violence, highlighting legal frameworks and proposing measures to combat this issue and protect victims in the digital realm.

Contents

Executive Summary

Digital violence against women is a growing challenge in light of the rapid and continuous advancement of information and communications technology. With the spread of the use of electronic means and social media applications, it has become easy for aggressors to exploit these tools to commit crimes of digital violence and harm women, especially since every citizen now has a smartphone connected to the internet and equipped with cameras and microphones, which has become one of the most commonly used tools to commit most digital crimes.

Digital violence is defined as the use of digital technology to engage in violent acts that harm individuals. This includes digital harassment, online threats, digital defamation, violations of digital privacy, and other forms of digital violence. Digital violence has negative impacts on victims, who are often women, including psychological, social, and economic impacts.

In the face of these challenges, the international community hastened to develop strong and effective international strategies and agreements to address the phenomenon of digital violence against women, which has become a serious violation of human rights, and to ensure the necessary and adequate protection of women. Some countries have also realized the importance of enhancing protection for women in the digital space and ensuring that they are not exposed to digital threats and harassment, and they have organized their legal framework in accordance with the provisions of these international agreements and taken the necessary measures and procedures to prevent violence and punish perpetrators.

Within this context, Lebanon issued a number of laws to address the problem of violence against women, protect their rights, and ensure their safety in real and virtual spaces. Therefore, a few laws were issued, including "the Law of Protection of Women and Other Family Members from Domestic Violence," the "Electronic Transactions and Personal Data Law," "the Criminalization of Sexual Harassment and Rehabilitation of Victims Law," and "The Trafficking in Persons Law." In addition to amending or adapting some of the basic laws in place, the most important laws are the "Lebanese Penal Code" and the "Law to Preserve the Confidentiality of Intelligence Conducted by Any Means of Communications," which made it possible for Lebanese judges to address relevant cases and punish crimes related to information technology through diligence in this regard. These laws allowed judges to hold criminals accountable. The most prominent example of this is when Lebanese jurisprudence considered that the element of publicity, which is a material element of the crime of defamation, is available if, for example, an e-mail is sent via the internet to several people. Hence, what if the act occurred through the use of Facebook and Instagram or other social media applications that are easy to hack and obtain access to personal data?

On the other hand, we have recently witnessed, according to officials' statements in Lebanon, a significant increase in cases of digital violence, especially those directed against underage girls, and their numbers have exceeded those reported to the security and judicial authorities. This is due to fear of shame and scandals, a lack of confidence in the judicial or security apparatus for prosecuting and following up on criminals, or a lack of awareness and knowledge about ways to report and prevent this type of crime.

This study aimed to analyze and understand this growing phenomenon of digital violence against women in Lebanon and to monitor development needs to combat digital violence and protect the rights of individuals in the digital space. This study also highlighted the legal and judicial reality in Lebanon

relevant to issues of digital violence against women, with a focus on how to address this issue and provide legal protection for victims of digital violence. In addition, it emphasized the role of security institutions in ensuring the protection of victims by prosecuting the perpetrators of these crimes; coordinating with civil society organizations to provide legal, social, and psychological assistance; and disseminating knowledge and awareness about the dangers of cybersecurity and ways to prevent information crimes.

This study also presented a set of recommendations to combat digital violence against women, including developing legislation that protects women's rights in the digital space, enhancing awareness and education about this phenomenon, and providing psychological and legal support to victims, in addition to strengthening international cooperation and cross-sector partnerships.

Forward

Artificial Intelligence as a Source of Strengths and Concerns

The most significant characteristic of contemporary civilization is the need for societies to establish mechanisms that safeguard individuals and groups by enacting general legislation and regulations that are binding as soon as they are approved. The foundation of these legislations and regulations rests on the Universal Declaration of Human Rights and the other international agreements stemming from it that form the Bill of Human Rights. Furthermore, the transformation from the rule of law to the rule of rights has become a fundamental objective for all societies striving to achieve modernity.

Accordingly, international and local legislative systems have undergone considerable development, which aligns with the challenges faced by societies. This legislative development is a response to the challenges faced by societies. Ironically, however, some of these challenges arise from the very progress that societies have made in scientific and technological inventions and innovations. These advancements have the potential to both enhance and hinder societies, as they increase the complexity of the issues that need to be addressed.

As the rapid advancement of technology continues to progress, it becomes increasingly clear that each invention or innovation carries certain threats that must be addressed. A current concern in the virtual world is the rapid development of information and communications technology, which has given rise to the emergence of artificial intelligence. This man-made tool, which has the potential to be weaponized against people, poses a significant threat to society. It was not until artificial intelligence began to spread false information and prey on humans that people became fully aware of the dangers it presented.

Recently, the domain of fabrication and victimization has had a significant impact on women, particularly those who actively participate in public life. The personal narrative and image of a woman have become subject to manipulation and attacks. Unfortunately, the prevalence of violence against women has taken a new form, which is the utilization of artificial intelligence to discredit and undermine women's dignity.

A new challenge has emerged for the legislative system: the need to issue laws and procedures that safeguard women from digital violence, particularly in the context of artificial intelligence. It is widely acknowledged that this concern holds significant importance for both the international legislative agenda and the priorities of national organizations that advocate for women's rights.

This research represented a precise scientific endeavor in monitoring both reality and risks. Beyond a shadow of a doubt, it served as a precursor to a new regulatory framework in a contemporary world that has expanded its capabilities and, consequently, its concerns.

Dr. Fadia Kiwan
Director General of the Arab Women's Organization

Introduction

The objective of this report was to conduct a research study that examined the current legal landscape in Lebanon and its approach toward addressing issues of violence against women on the internet. This report provides a summary of key judicial rulings made by Lebanese courts regarding cases of violence against women in the digital space. Additionally, the report analyzed the main trends of official and civil institutions that address discrimination and violence against women. The report offered recommendations to prioritize future efforts in developing the legal framework to protect women's rights to equality, justice, and participation in all fields, as well as to eliminate all forms of discrimination against women through advocacy and awareness campaigns.

The pervasive crime of violence against women is one of the most egregious human rights violations, affecting women universally, without regard to age, race, religion, culture, or socioeconomic status, across diverse countries and regions, and throughout various historical periods, whether in contexts of conflict and strife or in contexts of tranquility.

The criminal act of violence against women comprises a variety of forms of offenses, which encompass physical, sexual, and psychological assaults perpetrated against women in familial settings, public life scenarios, and instances where the state is complicit or condones such violence. These offenses include domestic violence, sexual harassment, rape, blackmail, threats, defamation, bullying, physical assaults with the intention of exploitation, and instances of human trafficking.

According to the United Nations,[1] violence against women encompasses any act of gender-based violence that results in, or is likely to result in, physical, sexual, or mental harm or suffering to women, including threats of such acts, coercion, or arbitrary deprivation of liberty, whether occurring in public or in private life.

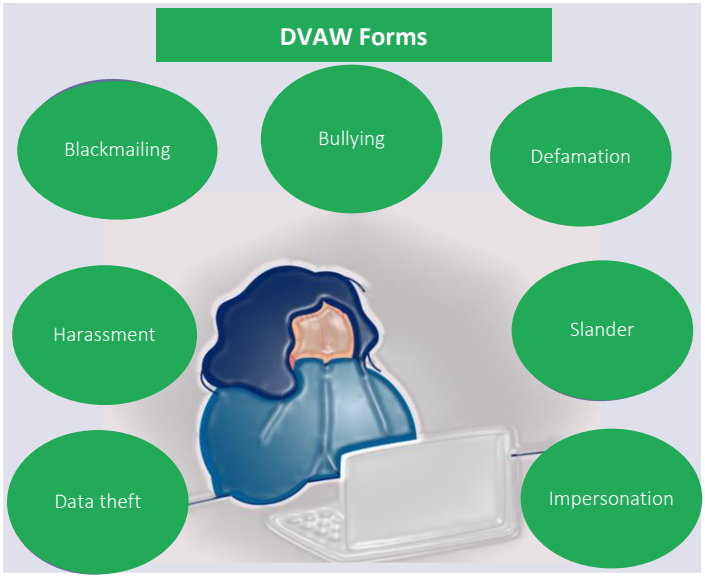
According to global estimates reported in a recent World Health Organization (WHO) publication,[2] 1 in 3 women, approximately 736 million women, or 35% of women worldwide, are subjected to physical or sexual violence throughout their lives. Such violence often leads to a range of physical and psychological problems for women, some of which may prove fatal, a figure that has remained largely static over the past decade. Moreover, this report revealed that 6% of women globally have experienced sexual assault from someone other than their spouse. However, due to the high level of stigma surrounding sexual assault and underreporting, the true magnitude of this issue is likely to be significantly greater than previously reported.

The proliferation of information technologies and the extensive use of the internet, which has become universally accessible with its capacity for data exchange and rapid communication with millions from around the globe through diverse social media platforms, especially with the prevalent utilization of smartphones and the plethora of services they offer in this regard, most notably capturing images and videos and the capability to disseminate them online. The issue of violence against women has transcended the physical realm and become a global phenomenon with severe ramifications for societies and economies worldwide. Despite the plethora of advantages provided by the advancement

[1] Declaration on the Elimination of Violence against Women- United Nations General Assembly Resolution No. 104/48 of 20 December 1993.

[2] Devastatingly pervasive: 1 in 3 women globally experience violence.

of information technology, cyberspace has emerged as a vast and boundless arena for acts of violence against women and girls. The risks associated with increased internet usage have escalated precipitously, particularly in the aftermath of the COVID-19 pandemic, which involves violations of privacy, blackmail, bullying, electronic harassment, and nonconsensual sexual messages.



Amnesty International has defined digital violence against women[3] as encompassing "various forms, including direct or indirect threats of physical or sexual violence; abuse targeting one or more aspects of a woman's identity, such as racism or transphobia; targeted harassment; privacy violations such as doxing (uploading private identifying information publicly to cause alarm or distress); and the sharing of sexual or intimate images of a woman without her consent. The aim of this violence and abuse is to create a hostile online environment for women with the goal of shaming, intimidating, degrading, belittling and ultimately silencing them."

In this study, we adopted a descriptive analytical methodology to assess the Lebanese legal framework pertaining to digital violence against women. We also reviewed pertinent judicial rulings and evaluated the extent to which they address the issue of digital violence against women and the legal protections offered by the Lebanese judiciary in this domain. Furthermore, we explored the role of national institutions and civil society organizations in providing legal assistance, safeguarding against cybersecurity risks, and promoting awareness and knowledge about preventing cybercrimes.

A systematic comprehensive approach was implemented to gather information and data pertaining to digital violence against women through a series of steps, the most significant of which are as follows:

- Multiple interviews were conducted with representatives from the security sector, including the Office for Combating Information Crime, judges, legal professionals, members of the public, and civil society organizations, led by the Women's Committee of the Bar Association.[4]
- Desktop research was conducted through the exclusive library of the Arab Center for the Development of the Rule of Law and Integrity[5] to collect legal texts, studies, and reports pertaining to the subject.
- Online research can be conducted through the internet and the websites of national institutions and civil society organizations to acquire additional information and corroborate the data gathered from interviews. This process involved reviewing prior studies, reports, and pertinent articles.

[3] Review of Amnesty International's report "Online violence against women in 2018."

[4] I extend my sincerest appreciation to all those who have contributed to the development of this report by providing relevant data and information during special individual meetings on this topic, specifically Dr. Fadia Kiwan, MP Cynthia Zarazir, activist Josephine Zogheib, Ms. Asmaa Hamada, activist Hayat Murshad, Mr. Charbel Al-Qarih, Mr. Charbel Shabir, and Ms. Jan Akl.

[5] The Arab Center for the Development of the Rule of Law and Integrity is a nongovernmental, nonprofit organization that was established in 2003 by a group of experts in the rule of law, judges, lawyers, and university Ms.s from several Arab countries. The Center's primary objective is to promote the principles of the rule of law and justice in the Middle East and North Africa region as a fundamental requirement for reform and democratic, social, and economic development. Interested individuals can learn more about the Arab Center's activities and projects by visiting its website at www.arabruleoflaw.org.

Digital Dimension of Violence Against Women and its Ramifications

The digital dimension of violence against women encompasses any act of gender-based violence directed at women that is facilitated, abetted, or aggravated by the use of various forms of information and communication technology, including but not limited to smart mobile phones, the internet, social media platforms, email, GPS tracking devices, offline drones and recording devices, and artificial intelligence. The purpose of such acts may be to insult or degrade a woman solely because of her gender, or they may result in negative consequences that disproportionately affect women compared to men.[6]

There are various forms of violence against women that can occur through the use of technology or the internet. The most prevalent of these are typically classified into four distinct groups:

1. Forms of harassment, violence, or mistreatment facilitated by specific technologies or devices, such as spyware or other tracking tools used by an intimate partner to commit acts of violence.
2. Abuse that occurs and is amplified online, such as the posting of nonconsensual intimate photos or other forms of image-based sexual assault.
3. The use of new forms of abuse, such as the publication of pornographic materials using deepfake technology or the misuse of digital selves in the Metaverse.
4. The use of digital space to commit acts of violence and abuse, such as the promotion of various forms of sexual violence against women through social media.

Violence against women via the internet or through technology encompasses a broad range of behaviors. These include 1) all forms of image-based sexual assault, such as the creation, publication, distribution, and sharing of images, video clips, or audio clips of a sexual or intimate nature on the internet without the victim's consent, as well as "deepfake pornography" created by artificial intelligence applications; 2) unauthorized access, manipulation, or distribution of personal data, such as data harvesting; 3) identity theft or impersonation, such as creating fake profiles; 4) acts that harm a person's reputation or credibility; 5) monitoring someone, such as cyberstalking; 6) online sexual harassment; 7) cyberbullying; 8) online sexual and physical threats and abuse; and 9) harassment and abuse of digital selves, such as avatars.

Among the significant criminal actions that may result from behaviors leading to digital violence against women, which are categorized as cybercrimes according to the report of the General Directorate of Lebanese General Security on information security and risk awareness,[7] we mention the following, which are relevant to the topic of our research:

- Digital Sexual Harassment: Article 1 of Law No. 205/2020 (Criminalizing Sexual Harassment and Rehabilitating its Victims) defines sexual harassment as “Any repeated bad behavior that is out of the ordinary, unwanted by the victim, with a sexual connotation that constitutes a violation of the body, privacy, or feelings of the victim, wherever they are, through sexual or pornographic words, actions, gestures, suggestions, or insinuations, and by any means of harassment, including electronic means. It also includes every act or endeavor, even if it is infrequent, that uses any type of psychological, moral, material, or racial pressure that aims to obtain a benefit of a sexual nature for the perpetrator or others.”

[6] The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform.

[7] To view the report of the General Directorate of Lebanese Public Security on information security and risk awareness, please review this electronic link: https://www.general-security.gov.lb/uploads/cyber_awarness_booklet.pdf

- Digital Extortion: This offense is characterized by the act of menacing and intimidating the victim through the publication of photographs or visual materials (video clips) or the disclosure of sensitive information about the victim, with the intention of coercing the victim into paying sums of money or compelling the victim to engage in unlawful activities for the benefit of the extortionists. Typically, victims are contacted through electronic mail or social media platforms. One of the primary motivations behind this crime is the acquisition of financial gain, as well as the dissemination of confidential information and the commission of immoral acts.
- Human Trafficking: This is the act of deceptively or coercively luring individuals with the intent of transporting them across national or territorial borders, depriving them of their autonomy and freedom. These individuals are often subjected to various forms of physical and psychological abuse. The advent of the internet has facilitated human trafficking operations by breaking geographical barriers and promoting the advertisement of criminal gangs. The objectives of human trafficking include forced labor, sexual exploitation, and the trafficking of human organs.

The Office of Cybercrime and Intellectual Property within the Internal Security Forces (ISF) of Lebanon[8] has reported that the majority of cybercrimes involve theft of electronic data, threats, sexual and physical blackmail, and defamation or electronic defamation and affect both men and women. Nevertheless, such crimes are frequently directed at women and girls in particular, as indicated by the Cybercrime Office. It is noteworthy that cases of cyberbullying have risen in Lebanon in recent years, particularly with the expansion of distance education. However, not all instances of cyberbullying are considered criminal. Many of these cases fall under the category of misdemeanors, but in some severe instances, they may be considered actual crimes.

> The General Directorate of Internal Security Forces – Public Relations Division disclosed a statement on May 4, 2020, indicating that during the implementation of the general mobilization decision, there was a significant rise in complaints of blackmail and sexual harassment crimes. Specifically, the number of reports increased by 184% compared to previous years. In 2018, the General Directorate of Internal Security Forces received 1,123 reports, while in 2019, the number of reports reached 1,270. However, from the beginning of 2020 until April, the General Directorate of Internal Security Forces recorded 315 reports.

In addition to defamation, reputation distortion, and slander, all of which are categorized as forms of digital bullying and are subject to legal repercussions as stipulated in the relevant legislation, particularly the Lebanese Penal Code, the Publications Law, and the Electronic Transactions Law.

[8] A statement issued by the General Directorate of Internal Security Forces- Public Relations Division and published on the Directorate's Facebook. A statement issued by the General Directorate of Internal Security Forces- Public Relations Division on May 4, 2020: During the implementation phase of the general mobilization decision, complaints of blackmail and sexual harassment crimes increased compared to the period before this phase, reaching:

122 complaints between the period extending from 2/21/2020 to 4/21/2020.

43 complaints between the period extending from 12/20/2019 to 2/20/2020.

Consequently, these crimes increased by 184%.

One of the most significant instances of defamation, threats, and digital blackmail in Lebanon are those directed at politically and/or socially active women, particularly those based on false and fabricated news, pictures, and videos. As the participation of women in political life in Lebanon increased, there have been numerous threats and defamation against them through various electronic means and social media, with the aim of insulting and discrediting them simply due to their gender. These cases are especially egregious because they seek to undermine the reputation and contributions of women who are actively engaged in the political domain.

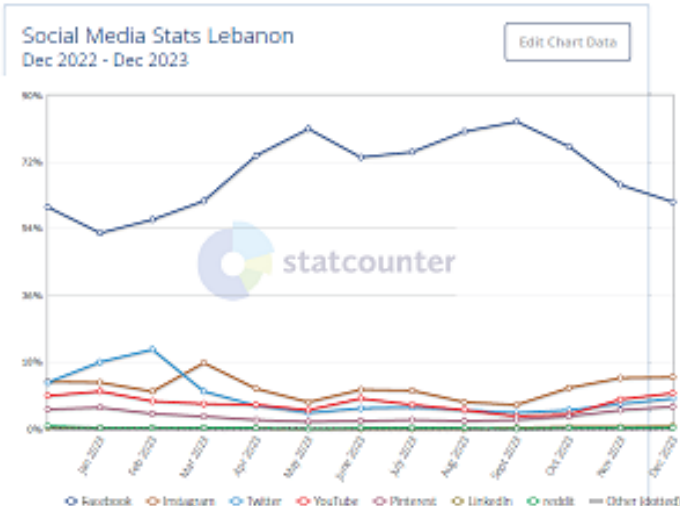
In a recent exclusive interview with Representative Cynthia Zarazir, a member of the Lebanese Parliament for the current parliamentary session (Parliament 2022), she recounted her experiences with digital violence. Specifically, she mentioned being the victim of false news stories, derogatory language, and moral violations that were published on social media platforms, such as Twitter and Facebook. Additionally, she claimed to have experienced threats of physical harm, including being beaten. She added, "If I were a man, I would not have been subjected to such mistreatment, and no one would have dared to threaten me with harm." Upon being inquired about prior complaints lodged with the competent judicial authorities, she stated, "I have submitted numerous complaints to the competent judicial authorities, but I did not receive any response from them, and thus, I ceased filing such complaints and opted to refrain from publishing the news and instead gather them to avoid punishment." The representative expressed regret for the current situation and stated, "Nothing will change as long as the patriarchal society prevails and as long as those in power are men. Legislation alone is insufficient; instead, efforts must be made to fundamentally alter the mentality and social behavior rooted in the patriarchal system by intensifying awareness campaigns and promoting full equality in schools and universities, as well as incorporating it as an educational subject within the curricula."

> “I was subjected to coercion and intimidation through the use of menacing and derogatory language, and malicious rumors were circulated and disseminated about me, in addition to manipulated video footage being broadcasted on social media platforms.”

According to Ms. Josephine Zogheib, a member of the Kfardebian Municipal Council, political and social activist, and former parliamentary candidate, she has faced numerous instances of violence, both digital and nondigital, as well as blackmail and threats during and after her candidacy for the Lebanese parliamentary elections. False information and edited video clips were also disseminated on social media platforms, particularly after she filed an appeal against the election results with the Lebanese Constitutional Council. Furthermore, she was subjected to an attempt to harm her when someone unbolted her car's wheels. Despite filing a lawsuit with the judicial authorities, she has not received justice. Ms. Zogheib emphasized the need to provide adequate protection to female politicians in Lebanon, who are frequently subjected to defamation and threats that can sometimes pose serious risks to their safety. She also stressed the importance of strengthening the Office for Combating Information Crimes to swiftly prosecute perpetrators of such crimes.

> “We must work to radically change the mentality and social behavior rooted in the patriarchal system.”

The proliferation of social media use has led to a considerable rise in instances of this type of offense, particularly given that access to such platforms has become widespread. Social media's impact on society is undeniable, as it has garnered the attention of various groups, particularly young people, who consider it an integral part of their lives. Notably, social media platforms significantly influence the perspectives, behaviors, and actions of younger generations.



A study conducted by Statcounter - GobalStats[9] from December 2002 to December 2023 revealed that the utilization of social media platforms in Lebanon was predominantly distributed among Facebook and Instagram users. The proportion of users for Facebook reached 61.46%, trailed by Instagram, where the proportion of users was 13.6%. Additionally, the usage rate of YouTube in Lebanon was 9.58%, followed by other platforms such as X-Twitter, Pinterest, and LinkedIn. Furthermore, LinkedIn and other social media platforms were used.

[9] To view the report issued by Statcounter-GobalStats.

Legal Framework for Cases of Digital Violence Against Women

In this section, we examined the legal framework pertaining to digital violence against women. The first part of this section focused on the international agreements that address this issue, as well as the agreements to which Lebanon is a signatory and/or has ratified in its effort to combat violence against women. The second part delved into the Lebanese legal texts that specifically address digital violence against women.

International and Regional Agreements

Violence against women is widely regarded as one of the most pressing and significant issues in contemporary societies, as it constitutes a grave infringement of human rights and presents formidable challenges that demand international strategies and accords to remedy them. In light of this, it has become imperative for the international community to band together and establish robust and effective international agreements that guarantee necessary and suitable protection for women. Consequently, international agreements have emerged as indispensable instruments for safeguarding the rights and welfare of women across the world, erecting an international legal framework that mandates countries to ratify it, working toward drafting legislation and regulations, and undertaking the requisite measures to prevent violence and hold perpetrators accountable.

Accordingly, various international and regional organizations have put forth several agreements with the aim of bettering the situation of women, achieving gender equality, and safeguarding them from violence. It is crucial for member states to transform these agreements into efficient national laws and policies and fortify the mechanisms for their effective implementation. Furthermore, the international community has made efforts to bolster international collaboration, with the goal of sharing experiences and offering support to countries in effectively implementing these agreements (see Appendix 2, List of international and regional agreements).

In response to developments and changes in the digital world, various bilateral, regional, and multilateral treaties have been drafted to address cybercrimes, including those committed through electronic media or the internet, including digital violence against women. The following are some of these treaties:

- The International Labor Organization Convention on the Elimination of Sexual Violence and Harassment (2019) pertains to the issue of workplace violence and harassment that occurs during work-related communications, including those facilitated by information technology. This convention defines "the term 'violence and harassment' in the world of work refers to a range of unacceptable behaviors and practices, or threats thereof, whether a single occurrence or repeated, that aim, result in, or are likely to result in physical, psychological, sexual or economic harm, and includes gender-based violence and harassment."
- The Council of Europe Convention on Electronic Crime, established in Budapest (2001), is designed to safeguard society from cybercrimes and has the potential to utilize computer networks and electronic information to perpetrate criminal activities. Specifically, it addresses concerns related to copyright infringements, computer and personal data fraud, child pornography, hate crimes, and network security breaches.

- The Arab Convention on Combating Information Technology Offences (2010)[10] aimed to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes to protect the security and interests of the Arab States and the safety of their communities and individuals. Crimes include pornography-related offenses and other crimes connected to pornography, as well as crimes involving the manipulation of data integrity and the misuse of information technology resources. Furthermore, the convention addresses the crimes of fraud and invasion of privacy through the use of information technology.
- The Beijing Declaration, which was ratified in 1995 following the Fourth World Conference on Women, where more than 40,000 government representatives, experts, and civil society members convened, ensures the protection and empowerment of women by enhancing their proficiency, knowledge, and access to information technology. Consequently, it aims to increase women's participation and enable them to express their viewpoints and make decisions in the media and new communication technologies.

However, Lebanon, despite the importance of the issue of digital violence and its widespread spread, has not yet officially signed the Budapest Convention on Cybercrimes, the Arab Convention to Combat Information Technology Crimes, or the International Labor Organization Convention on the Elimination of Violence and Sexual Harassment. Despite this, the government has enacted legislation and procedures to combat cybercrimes and protect male and female citizens from information and communications technology-related issues, in accordance with the principles and objectives of the Budapest and Arab conventions. Lebanon has also updated national laws and strengthened cooperation with the international and regional community in this regard. For instance, the Law on Combating Cybercrime and Protecting Intellectual Property and the Law on Preventing Sexual Harassment No. 205/2020 were introduced to address these issues. These laws are discussed in more detail in the following sections.

Lebanon ratified the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) through Law No. 572/96, which was enacted on July 24, 1996. This ratification has led to increased awareness of women's rights in Lebanese society and fostered the advancement of gender equality and women's empowerment in various economic, political, and social fields. However, the ratification did not guarantee women their full rights, and it did not ensure their absolute equality with men, especially considering the reservations that Lebanon has on some articles of the agreement, such as Article 9, paragraph (2), which pertains to a woman's right to grant her children nationality, and Article 16 (1) (c), (d), (f), and (g), which addresses personal status and stipulates equal rights in marriage, the rights of the mother in matters related to her children, guardianship, and adoption of children and regarding the family name. Additionally, there is Article 29, paragraph (1), which pertains to the settlement of disputes related to the interpretation of the Convention before the International Court of Justice.[11]

It should be highlighted that Lebanon has refrained from signing the Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), which enables state parties to lodge grievances with the CEDAW Committee concerning breaches of women's rights and acts of violence against women.

In 1971, Lebanon ratified the United Nations Convention on the Elimination of All Forms of Racial Discrimination (CERD), which aims to eradicate all forms of racial discrimination, including violence against women resulting from racial discrimination.

[10] The Arab Convention on Combating Information Technology Offences of 2010.

[11] The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW).

Moreover, the Lebanese Republic has committed to a range of international agreements that specifically criminalize instances of violence against children and women. Among the most significant of these agreements are the following:

- The International Convention on the Political Rights of Women, which Lebanon ratified on February 24, 1954, according to a law issued on November 29, 1955.
- The Convention on the Rights of the Child was ratified by Lebanon on May 14, 1991.
- The Optional Protocol to the Convention on the Rights of the Child concerning the participation of children in armed conflicts, which Lebanon ratified on February 11, 2002.
- The Optional Protocol to the Convention on the Rights of the Child, which pertains to the sale of children, their exploitation in prostitution, and the production of pornographic materials, was ratified on November 8, 2004.
- The Convention against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment was ratified on December 22, 2008.
- The International Covenant on Economic, Social, and Cultural Rights was ratified on November 3, 1972.
- The International Covenant on Civil and Political Rights was ratified on November 3, 1972.
- On December 18, 2001, the government of Lebanon, represented by its Ambassador to the United Nations, formally acceded to the United Nations Convention against Transnational Organized Crime by signing the requisite instrument.
- Authorizing the government based on Law No. 682 of August 24, 2005, to join the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime.
- Authorizing the government to join the Arab Charter on Human Rights, which was signed in Tunisia on May 23, 2004, in accordance with Law No. 1 of 2008. It guarantees women equal rights and human dignity, safeguards them from all forms of violence and abuse, and ensures nondiscrimination between men and women in the right to equally benefit from training, employment, labor protection, and wages when the value and quality of work are equal.

Legal Texts Pertaining to Digital Violence Against Women in Lebanon

Lebanese law is committed to safeguarding the privacy and personal freedom of individuals. This principle is enshrined in the Lebanese Constitution of 1926, which includes provisions for the protection of privacy in Articles 8 and 13. Article 8 specifies that "personal freedom is protected by the law," while Article 13 protects the right to freedom of expression, the right to access information, and the right to privacy in all forms of communication. Additionally, the Constitution emphasizes the principles of equality between men and women, with provisions in Article 7 stating that "all Lebanese are equal before the law and enjoy equal civil and political rights."

The Constitution, with its unequivocal language, underscores the obligation to honor international agreements, as evidenced by the following passage in its preamble: “it is a founding active member of the United Nations Organization, committed to its Charter and the Universal Declaration of Human Rights. The State embodies these principles in all sectors and scopes without exception." This extends to all governing bodies the duty to fulfill their responsibilities to the international community by observing international conventions.

The Lebanese legislature has established legal texts protecting citizens' right to privacy and the right to access information through all forms of communication. These protections extend to cases of violence committed against women, which can take the form of physical or sexual assault, as well as moral

violence that may have a negative impact on the victim's mental and emotional well-being. This includes any acts of defamation or slander that may harm the victim's dignity or reputation. Furthermore, the legislation also covers any threats made against the victim, which can have a significant impact on their mental and emotional state.

Therefore, the Lebanese Penal Code includes provisions that penalize acts of violence regardless of the gender of the perpetrator or victim. These provisions apply to acts of violence committed through the internet or by other electronic means. In addition, Lebanon has enacted specific legal texts to address cases of violence against women.

In light of the ongoing information technology revolution, it has become essential for countries to enact legislation and regulatory measures to regulate digital transactions, safeguard cybersecurity, and combat various forms of cybercrimes, including those that target women and children, particularly those involving pornographic content. Given the proliferation of artificial intelligence and its diverse applications, which have significantly eroded the sanctity of private life and invaded individual privacy, new forms of cybercrimes have emerged, with digital violence against women and children being among the most pressing concerns.

In 2009, the Economic and Social Commission for Western Asia (ESCWA) introduced the "Guidelines for Cyber Legislation for ESCWA Member States,"[12] which encompassed six guidelines: 1) The first guideline focused on electronic communications and freedom of expression; 2) The second guideline pertained to electronic transactions and electronic signatures; 3) The third guideline addressed e-commerce and consumer protection; 4) The fourth guideline concerned processing and protection of personal data; 5) The fifth guideline dealt with cybercrimes; and 6) The sixth guideline covered intellectual property rights in the information and cyber fields. The purpose of these guidelines was to provide a reliable legal framework that ESCWA countries could use when drafting their own electronic legislation.

Lebanon has released a range of legal documents aimed at regulating cybersecurity and addressing cybercrimes. While this response may be seen as tardy in comparison to certain Arab countries, such as those where the Electronic Transactions Law was introduced in 2018, it remains a significant step in the right direction.

We identified and presented the legal texts that pertain to the subject matter of our research below. These legal texts are categorized into two sections: the first section encompasses the legal texts that have a direct connection to digital violence against women, while the second section comprises indirect legal texts that pertain to digital violence against women.

[12] The Arab Center for the Development of the Rule of Law and Integrity was responsible for developing these guidelines, under the supervision of Dr. Wassim Harb, founder and general supervisor- senior advisor in legal informatics. The guidelines were commissioned by the United Nations Economic and Social Commission for Western Asia- ESCWA in 2009, with the aim of assisting Arab countries in developing national cyber laws and coordinating cyber legislation at the regional level. The ESCWA guidelines for cyber legislation were reviewed in the process.
https://archive.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf

Legal Texts That Specifically Address Digital Violence Against Women

- Law No. 205 of December 30, 2020, was enacted to **criminalize sexual harassment and provide support for its victims**. The law offers a comprehensive definition of sexual harassment as "any bad and repetitive behavior that is out of the ordinary and unwanted by the victim and has a sexual connotation that constitutes a violation of the body, privacy, or feelings that occurs against the victim wherever she is, through sexual or pornographic words, actions, gestures, or insinuations." The law indicates that sexual harassment occurs by any means, including electronic means. The law considers sexual harassment "as any act or attempt that employs psychological, moral, or racial pressure to obtain sexual benefits for the perpetrator or others, regardless of whether it is repeated or not." The law encompasses all forms of sexual harassment, including those perpetrated through electronic means such as the internet. Law 205/2020 imposed penalties on perpetrators of sexual harassment crimes in various cases, including imprisonment from one month to one year and a fine of up to ten times the minimum wage. If the crime occurs within the context of a dependent or work relationship or in government agencies, universities, or military institutions, the penalties may increase to imprisonment for up to two years and a fine of up to twenty times the minimum wage. The punishment for this offense increases to imprisonment for up to four years and a fine of fifty times the minimum wage if the crime is committed against a minor or an individual with special needs. Additionally, if the harasser has any form of authority over the victim, such as in terms of material possession, moral standing, education, or employment, the penalty will be more severe. If there are multiple perpetrators or if the harasser uses psychological or moral pressure to coerce the victim into providing sexual favors, the penalty will also increase. The legal framework also comprises special provisions that prohibit infringing upon the rights legally guaranteed to victims of sexual harassment, particularly with respect to wages, promotions, transfers, renewals of work contracts, or imposing disciplinary penalties upon them. Furthermore, measures are implemented to safeguard the rights of victims of sexual harassment through the establishment of a dedicated fund at the Ministry of Social Affairs. This fund aims to help victims of sexual harassment and ensure their care to promote their rehabilitation and reintegration into society. The fund also provides avenues to minimize and prevent such crimes while rehabilitating the offenders.
- Law No. 81 of October 10, 2018, **the Electronic Transactions and Personal Data Protection**, was enacted to provide a comprehensive legal framework for the protection of personal data in its fifth chapter. This chapter outlines the objectives and controls for processing personal data, including the types of processing that are prohibited by law. It also specifies the procedures for collecting personal data and the responsibilities of the data controller. Chapter Six addresses crimes related to information systems, data, and payment cards, as well as some amendments to the Penal Code (Legislative Decree No. 340 dated 3/1/1943). This chapter includes penal provisions for crimes related to information systems and data, the forgery or imitation of payment or debit cards, and the failure to comply with the rules governing electronic commerce. Additionally, it covers special provisions for the exploitation of minors in pornographic materials and electronic forgery and electronic publishing. Chapter Seven outlines the procedural rules for seizing and storing information evidence, defining the digital evidence and information traces that the judicial police are required to seize and preserve.

  The Electronic Transactions Law, as stipulated in Article 119, characterizes electronic forgery as the deliberate alteration of verifiable facts or data, which is documented on an instrument, manuscript, paper, electronic, or any other medium that serves as a document, with the intention of causing material, moral, or social harm.

  Article 118 of the specified regulations outlines the provisions for publication by electronic means. It states that any form of visual content, including writing, drawings, paintings, photographs, films, badges, and others, that is displayed in a public place open to the public, sold, offered for sale, or distributed to one or more individuals through any approved means, including electronic means, is subject to these provisions.

  Article 120 of Law No. 81/2018 outlines criminal offenses related to the exploitation of minors in pornographic materials. According to the law, "the act of photographing, portraying, or representing any minor through drawings, pictures, writings, films, or signs, in a real or artificial manner, for the purpose of simulating explicit sexual activities or depicting the sexual organs of a minor, constitutes a crime." Penalties for such crimes are determined in accordance with the provisions of the Lebanese Penal Code,

specifically amended Articles 535 and 536, which mandate that "the production of pornographic content involving and exploiting minors in such materials is deemed a criminal offense (a crime of trafficking in persons) under Article 586 (1) and subsequent sections of the Penal Code, which pertains to trafficking in persons." In addition, Article 120 specifies that "anyone who habitually broadcasts or keeps pornographic materials related to the exploitation of minors via radio or television, communication services directed to the public, or any other means shall be punished with imprisonment for a maximum of one year and a fine of up to two million Lebanese pounds, or one of these two penalties."

Article 121 of the Electronic Transactions Law provides a definition for information evidence, which comprises digital or information evidence. These are described as "data that individuals voluntarily or involuntarily leave on systems, databases, information services, and information networks. Information evidence encompasses a wide range of categories, including information equipment, programs, data, applications, and other related artifacts. The provisions outlined in this chapter are to be followed when obtaining information evidence based on the decision of the public prosecution or the appropriate judicial authority. It is important to respect privacy when dealing with information effects, particularly in regard to data and images that are not relevant to the criminal case. The judicial police are responsible for carrying out the procedures for seizing and preserving information evidence, as outlined in this chapter, and based on the decision of the appropriate judicial authority."

The Electronic Transactions Law endows the competent judiciary and the specified authorities with the power to compel technical service providers to surrender data in their possession or control, as stipulated in Article 72 of Chapter Two, within the limits of investigation and trial requirements. The judicial police are authorized, in the context of criminal investigation procedures, to request that technical service providers retain additional technical data for a maximum period of thirty days, relating to a specific incident and individuals, given the urgency and potential for data loss or alteration. These data may only be accessed by the judicial police through a decision of the competent judicial authority, and technical data are subject to the professional confidentiality required by the technical service provider. However, the technical service provider may not invoke this confidentiality before the competent judiciary, subject to the constraints of investigation and trial requirements as outlined in Article 121, which states that "the seizure of informational evidence shall occur based on the decision of the Public Prosecution or the competent judicial authority."

It should be noted that the requirement for preservation does not extend to stored or transmitted content or material that reflects the sentiments of the individual who generated it, such as exchanged communication, or the information contained in stored or transmitted data or websites. The process for safeguarding data related to information movement and the particulars of this information or erasing it is defined by a decree issued by the Council of Ministers, guided by the proposal of the Minister of Justice.

Legal Texts Indirectly Pertaining to Digital Violence Against Women:

- The Lebanese Penal Code, issued by Legislative Decree No. 340 dated January 3, 1943, and its subsequent amendments remain applicable to numerous offenses committed through electronic means, despite the absence of specific information crimes within its provisions.[13]
    - The provisions of Articles 282 and 283 of the Penal Code establish that individuals who intentionally acquire, obtain, or retain documents or information outlined in Article 281 of the Penal Code with the intent to disclose them shall be subject to imprisonment. This may include electronic records or discs utilized in computer systems and thus may constitute criminal materials.
    - The Penal Code provides for the punishment of numerous cybercrimes committed through the dissemination of materials, images, or electronic messages over the internet that result in acts of violence against women and children, such as threats and blackmail, or pose a threat to public morals (Articles 531, 532, and 533). These crimes can also include the exploitation of minors in pornographic materials (Articles 535 and 536, as amended by Law 81/2018). The penalties for these offenses are specified in the Penal Code.

[13] Cybercrimes in light of Lebanese law and jurisprudence, intervention by Judge Fawzi Khamis- President of the Legal Informatics Development Association in Lebanon.

- The provisions of Article 536 in this law mandate increased penalties when the internet or any other electronic communication network is utilized to disseminate and circulate pornographic content featuring minors to a diverse and indeterminate audience.

> *Penal Code No. 140 dated October 27, 1999*
>
> Article 536 specifies heightened penalties for the use of electronic communications networks, such as the internet, to publish or distribute pornographic material related to the exploitation of minors, to an unspecified audience. This includes habitual capturing or reviewing of such material. The use of radio or television broadcasting, communication services directed to the public, or any other means to disseminate such material is also punishable by imprisonment for a maximum of one year and a fine not exceeding two million Lebanese pounds, or by either of these penalties. The provisions of this article apply to pornographic images of a person who appears to be a minor. If a legal entity is found guilty of committing the criminal act outlined in this article, they may also be subject to suspension from work for a period ranging from at least one month to two years.

- Criminalizing acts of defamation, slander, and threats that inflict harm, as outlined in Articles 582, 584, and 578, are crucial. These offenses, including those committed via social media platforms, are subject to penalties in accordance with Article 209. The penalties for such offenses have been amended in accordance with Article 118 of Electronic Transactions Law No. 81/2018, which has expanded the scope of publication to include electronic means. Given the current widespread use of the internet as a means of publication, it is now considered a public space that is accessible to the public, as described in the opening paragraph of Article 209 of the Penal Code.
- Furthermore, Article 650 of Penalties may be applicable in this situation, which penalizes individuals who threaten to expose, disclose, or report on a matter that would tarnish another person's reputation or honor to coerce them into obtaining an illegal benefit for themselves or others. This penalty can be imposed even if the information used in the threat or coercion is obtained through information systems, as the text does not specify the source of the information. Additionally, Article 655 allows for the punishment of fraud crimes that are committed through electronic means.

The Lebanese Penal Code provides for the punishment of certain crimes related to information technology. This is a result of the judicial jurisprudence of Lebanese judges, who aim to ensure that criminals are not able to evade punishment. The judiciary also seeks to address the challenges posed by rapid technological advancements by applying existing laws in an appropriate manner. However, it is suggested that relying solely on judicial jurisprudence to expand the application of existing laws may not be sufficient to keep pace with technological advancements. Therefore, it is recommended that the Penal Code be amended to incorporate updates that are commensurate with developments in information technology.

- Trafficking in Persons Law No. 164, enacted on August 24, 2011, amended the Lebanese Penal Code and added a new chapter to Chapter Eight of Book Two of the Penal Code. This law was implemented to fulfill Lebanon's international obligations related to punishing the crime of trafficking in persons. Article 586 (1) of the amended Penal Code outlines the penalties for the crime of trafficking in persons, which frequently targets women with the intention of exploiting them sexually or for financial gain. This exploitation is often facilitated through the use of various methods, including the employment of internet platforms such as social media, online marketplace websites, and existing web pages. Traffickers may also use fake advertisements and job postings to recruit victims and attract clients, offering enticing wages.

> *Penal Code No. 140, enacted on October 27, 1999*
>
> Article 586 outlines the punishments for the offense of trafficking in persons as a) luring, transporting, harboring, or confining an individual, b) employing force, coercion, deception, or taking advantage of a position of vulnerability to obtain or provide anything of value in exchange for the victim's labor or services, and c) with the aim of exploiting or facilitating his exploitation by others. It specifies that one of the forms of exploitation is forcing a person to participate in any of the following acts: a) committing an act punishable by law, b) engaging in or facilitating prostitution, or c) engaging in sexual exploitation.

- A law designed to safeguard the confidentiality of intelligence obtained through any form of communication, Law No. 140, was enacted on October 27, 1999, and later amended by Law No. 158 on December 27, 1999. This legislation was enacted to uphold the confidentiality of intelligence, as stipulated in the Lebanese Constitution, which is considered a fundamental human right. Additionally, the law aims to implement the provisions of the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, particularly Articles 12 and 16, which prohibit arbitrary or illegal interference with a person's privacy, residence, correspondence, or reputation and honor. This law establishes that the principle of intelligence confidentiality is protected by law and may only be violated under explicit circumstances that outline the principles and conditions for such violation. Violation of intelligence confidentiality through any means of communication, including landline or mobile devices, fax, or email, is prohibited. Furthermore, Article 17 of the law criminalizes illegal interception, with penalties of imprisonment for one to three years and a fine of 50 to 100 million LBP for anyone who intercepts any communication in violation of the law.

> *Intelligence Secrecy Law No. 140 dated October 27, 1999*
>
> Article 1 specifies: "Confidentiality of communication through wired or wireless means, including fixed telephone devices, mobile devices of all kinds, such as cellular, fax, and e-mail, is protected by law and not subject to any form of eavesdropping, monitoring, interception, or disclosure, except as specified in this law and through the means and principles outlined herein."

This legislation unequivocally delineates the circumstances in which it is permissible to breach the confidentiality of intelligence, which it views as an exception to the rule of confidentiality of intelligence. It also specifies the exceptional measure of intercepting telephone intelligence, either through a judicial decision or an administrative decision. In the event of a judicial decision, the law grants the Public Prosecutor at the Court of Cassation and the First Investigating Judge in each governorate the authority to make a decision requiring intelligence interception, provided that the exceptional measure targets a person suspected of being a perpetrator, accomplice, or accessory to a crime punishable by imprisonment for a period of no less than one year, with only information related to the crime included in the investigation file. In the case of an administrative decision, the law grants the Ministers of Defense and Interior, with the approval of the Prime Minister, the authority to decide requiring intelligence interception for the purpose of gathering information related to combating crimes against state security, terrorism, or organized crime. The intelligence is monitored by the security or administrative agencies specified by the minister in his decision, and a report is prepared that includes only the information covered by the intercepted intelligence and is related to the subject of the reason for the procedure.

- The Protection of Women and Other Family Members from Domestic Violence Law No. 293 of 5/7/2014, which amended the Lebanese Penal Code and was further amended by Law No. 204 of 12/30/2020, defines domestic violence as "any act, lack of action, or threat committed by a family member against one or more family members in accordance with the definition of family, involving one or more of the crimes set forth in this law and resulting in physical, psychological, sexual, or economic harm." This law establishes the criminalization of domestic violence and the penalties imposed on perpetrators, as well as the implementation of measures to protect victims. However, this law does not cover all cases of domestic violence, such as marital rape, and does not clearly specify the means by which the crime of domestic violence is committed.

Role of Judiciary and Security Agencies in Combating Digital Violence Against Women

The Role of the Judiciary in Adjudicating Cases of Digital Violence against Women

The judiciary in the Lebanese Republic has a crucial function in upholding public morals and safeguarding the family in a conventional sense that is compatible with Eastern customs and traditions, which are still highly valued socially and officially. There are several reasons for this, with perhaps the most significant being the patriarchal system that is prevalent in our Arab world. The sectarian system also unanimously supports maintaining the family in its traditional form, in accordance with religious teachings. As a result, any form of violation or crime that undermines public morals, dignity, and decency, particularly those affecting the most vulnerable groups such as women, children, and individuals with special needs, is strictly prohibited.

The judiciary is committed to taking necessary measures to investigate and prosecute perpetrators of crimes against vulnerable groups, with the aim of protecting these groups. This includes delving into investigations, whether traditional or technical in nature, to reach the perpetrators, arrest them, and refer them to the appropriate courts.

Public Prosecution, therefore, bears the responsibility of safeguarding society from crimes targeting specific groups, particularly when the victim is unable to defend themselves or engage in legal representation. In these cases, the prosecution initiates legal proceedings based on a complaint from the affected individual while adhering to the established rules and procedures. There has been a noticeable increase in the prosecution of such crimes over the last ten years, largely due to the widespread dissemination of information through the internet or the filing of complaints by affected individuals. This increase is also attributed to the enhanced capabilities and accuracy of investigative agencies, which have resulted in the apprehension, prosecution, and punishment of perpetrators.

Punitive measures resulting from legal proceedings for this type of lawsuit are designed to impose sanctions as outlined by statutory law. The judiciary also serves as a deterrent by adhering to the stipulated penalties and refraining from granting mitigating circumstances, except in rare cases. Furthermore, when a crime is committed using electronic communication means, such as the internet or smartphones, as specified in Article 536 of the amended penalties, punishment may be increased to prevent the proliferation of such crimes, which have become increasingly easy to commit due to technological advancements. As almost every citizen possesses a smartphone with internet connectivity and is equipped with cameras and microphones, which are commonly used to facilitate this type of crime, it is essential to enforce the stipulated penalties to deter potential offenders.

The judiciary takes great measures to maintain confidentiality throughout the investigation process, with the aim of protecting sensitive information that could cause moral harm to either the victim or the suspect and preventing defamation and the spread of rumors that may lead to prejudicial judgments and opinions.

Within this context, the judicial system in Lebanon operates in close coordination and collaboration with the Office for Combating Cybercrimes and Intellectual Property Protection, which is part of the Criminal Investigation Section of the Judicial Police. This office is responsible for investigating cases

involving digital technology or in which technological means are used to commit crimes, such as online threats and harassment, as well as defamation.

The aforementioned office, upon referral from the judiciary, conducts investigations aimed at identifying the perpetrator and determining the location of the crime, with the ultimate goal of applying the relevant articles of the Code of Criminal Procedure. This process is intended to determine the course of the case with regard to its form before the relevant authorities. Following this, the investigations are referred to the competent courts. The Lebanese judiciary, in collaboration with the Cybercrime Office, has been successful in apprehending a significant number of perpetrators of such crimes, particularly when committed within Lebanon or with the use of servers connected to the internet via data transmission companies based in Lebanon.

The Lebanese judicial system works in collaboration with international organizations, such as Interpol, to gather and maintain digital evidence. Additionally, it cooperates with local and international communication companies that offer internet services, including those that manage websites or applications facilitating communication between users. Known as technical service providers, these communication companies play a crucial role in obtaining data that can reveal important digital evidence, such as the identity of the perpetrator, the time and location of the crime, and other relevant information. Law No. 81 of 2018 requires technical service providers to retain information that identifies each subscriber and to store digital data traffic, excluding content, for a period of three years. This legislation also empowers the judicial police to request that service providers preserve specific or additional digital data for 30 days, with the approval of the court. These service providers are legally bound to comply and provide all necessary assistance.

Electronic Transactions and Personal Data Law No. 81, enacted on 10/10/2018

Article 72: It stipulates that technical service providers must retain information about the movement of data for all individuals who use their services, which can be used to identify them, as well as other technical data related to communication, for a period of three years starting from the date of service implementation.

In the context of criminal investigations, the judicial police may, after informing the appropriate judicial authority, request that technical service providers preserve additional technical data for a maximum of thirty days, in relation to a specific incident and identified individuals, due to the potential for data loss or modification. This data may only be provided to the judicial police by a decision of the competent judicial authority. It is important to note that the requirement to preserve data does not extend to stored or transmitted content or content that expresses the ideas of the individual who created it, such as exchanged messages or the content of stored or transmitted information or websites.

The legal system allows judicial authorities to seek the assistance of experts when needed, as stipulated in Article 34 of the Code of Criminal Procedure No. 328, which was enacted on February 8, 2001. This provision grants the Public Prosecutor the power to request the services of one or more experts, either during the course of the investigation or outside of it, to examine complaints or news and to utilize their specialized knowledge. The legislature did not specify the nature of the expertise needed, and therefore, there is no legal impediment to seeking the assistance of experts in the digital realm to authenticate digital evidence and aid judges in their deliberations.

In contrast, the judiciary actively collaborates with national organizations and pertinent associations to safeguard women and other vulnerable groups. This cooperation encompasses supporting victims and pursuing cases in the aftermath of the crime's occurrence.

In 2000, the Lebanese judiciary, in collaboration with international institutions, resolved a criminal case involving a severe moral violation that occurred on the internet. The Lebanese security authorities, aided by Interpol, apprehended a Lebanese national who was disseminating and distributing pornographic images of minors online at the behest of the prosecution. The public referred the individual to the investigating judge in Beirut, who subsequently issued an indictment against him under Articles 531, 532, and 533 of the Penal Code. The single criminal judge in Beirut then convicted him based on these articles and sentenced him to imprisonment and a fine. However, the Court of Criminal Appeal subsequently overturned and partially invalidated the ruling, as it determined that the elements of the two crimes outlined in Articles 531 and 532 of the Penal Code were not met due to the absence of the publicity requirement specified in Article 209 of the Penal Code. Nevertheless, the court convicted him under Article 533 of the Penal Code.[14]

Therefore, the issue at hand pertains to the availability of publicity[15] through the internet and social media. While the Criminal Court of Appeal's decision may differ, many legal researchers and judges concur that the internet has emerged as a critical means of global, regional, and local publishing. Indeed, it is widely regarded as a public space that is open to the public, as stipulated in Article 209 of the Penal Code. Consequently, it is an essential component in determining the applicable penalty for a crime, which has been refined and increased under Article 536 of the Amended Penal Code. However, it is important to note that the availability of the crime itself is not impacted by this factor.

In accordance with Lebanese jurisprudence, there has been a consistent approach in this matter. This is because the act of defamation specified in Article 386/1 has been deemed to have sufficient components, and it is considered to be a crime that takes place via the internet. It has been ruled that those who commit such crimes should be convicted based on the availability of the material element of the crime, which involves attributing a specific matter to a person who harms their honor or dignity on the internet, as well as identifying the individual to whom the slander is directed.[16]

With regard to the provisions of Article 209 Penalties, case law has determined that sending an electronic mail via the internet to numerous individuals falls within the scope of the stipulated cases. What if the act was carried out through Facebook, Instagram, or other social media platforms that are easily susceptible to hacking and accessing their data? In such instances, whoever publishes any content that includes disparaging, insulting, or defamatory language, whether in written, audio, or visual form, through social media platforms, such as Facebook, Instagram, and Twitter, would be considered to have committed the crime of libel and defamation, the penalty for which is severe due to its public nature, regardless of whether the actor's account is private and not intended for public viewing.

In the context of traditional crimes, it is necessary to establish and verify the perpetrator's identity before the perpetrator can be prosecuted and held accountable. However, determining the identity of

[14] Cybercrimes in light of Lebanese law and jurisprudence, intervention by Judge Fawzi Khamis- President of the Legal Informatics Development Association in Lebanon.

[15] Publicity constitutes what is meant by the attribution being made publicly." The Publications Court considered that the crime of public defamation is achieved as a result of the presence of three elements: the existence of an incident that was attributed to the victim, that this attribution would harm the honor and reputation of the victim, and that it was disclosed publicly. (Publications Court Decision No. 58 dated 11/13/2000, published in Al-Adl Magazine, issue 2001, page 336).

[16] Crimes of defamation and slander via the internet, a study by lawyer Samer Oweidat https://saderlaw.com/.

a cybercriminal can be a more intricate process, as its virtual digital identity encompasses a broader range of elements than their real-life identity. Therefore, identifying the criminal requires not only knowing the digital identity of the individual being pursued but also linking that identity to their legal identity as a real person. Additionally, it is crucial to determine whether the digital identity in question, which is associated with electronic technical elements, is indeed the one that committed the crime. To determine the identity of a cybercriminal, new and unfamiliar elements may enter the physical world, such as contact data and the internet Protocol address (IP Address), which is a critical piece of information that can lead to the identification of the user.[17]

Thus, the inquiry seeks to establish the IP address to determine two key factors: first, the geographical location of the individual in question, thereby addressing the issue of the court's spatial jurisdiction; second, identifying the subscriber of the internet service and resolving the question of whether the subscriber and the user of the IP address are one or the same person. This is crucial in determining the identity of the individual who committed the act and the service user.

This issue may occur when it becomes evident that the IP address is associated with public computers, which are utilized by multiple individuals (for instance, in cafes that allow customers to access the Wi-Fi calling service). In this instance, we delve further into the examination of digital data, encompassing factors such as the timing of service utilization, the specific applications/websites accessed, and personal accounts on social media platforms. To this end, we collaborate with the management of these digital platforms and social media companies to determine the postal address or cell phone number associated with the access and subsequently query the cellular companies' database to obtain information on the owner of the number. If there are grounds for suspicion, measures such as emptying the phone or laptop memory may be taken to confirm the files deleted by the suspect, and should they still exist, they would be retrieved and treated as digital evidence.

Law No. 81/2018 established the process for investigating electronic devices of suspects. The technical work associated with these means commenced upon the enactment of the aforementioned law in late 2018.

The judiciary in Lebanon has attempted to address this issue, and the judicial police have opted to employ the "funnel or hourglass" method in their investigation. This approach commences with the acquisition of the most pertinent information, such as the IP address, subscriber identity, cell number, and e-mail address, to ascertain the user's identity and associated data. Additionally, the method involves examining the individual's mobile phone or laptop to determine their place of residence or the location of the crime, thereby establishing the applicable jurisdiction and the potential for prosecution. If the individual is found to be involved in the crime, they may be arrested, interrogated, or subject to electronic monitoring to facilitate their apprehension.

In terms of jurisdiction, the Lebanese legislature established the spatial jurisdiction of the Lebanese judiciary in accordance with Article 15 of the Lebanese Penal Code. This article stipulates that a crime is considered to have been committed on Lebanese territory in two cases: A) if one of the elements that constitutes the crime, or an act of an indivisible crime, or an act of primary or secondary association, is committed on this land; or B) if the result occurred on this land or was expected to occur on it. Therefore, the issue of territorial jurisdiction of the Lebanese judiciary arises when one of the elements of the crime was committed outside of Lebanese territory or if its elements were distributed

[17] The problem of determining the identity of the cybercriminal and his place of residence on social networking sites, a study by lawyer Charbel Al-Qarih. Doctor of Laws. Former Chairperson of the Informatics Committee at the Beirut Bar Association.

among more than one country. However, there is no issue if all the elements of the crime occurred in Lebanese territory, such as a person residing in Lebanon accessing the information system of another person in Lebanon and threatening or blackmailing them financially. In this case, all the elements of the crime would have occurred in Lebanese territory. Consequently, the Lebanese legislature has defined the cases of territorial jurisdiction of the Lebanese judiciary:

1. Any of the components of a crime have been carried out within Lebanese territory.
2. A single, indivisible act of a crime has been committed within Lebanon territory.
3. The primary or secondary act of participation took place in Lebanese territory.
4. Whether the criminal outcome or its intended occurrence (i.e., the criminal attempt) transpired or was anticipated to take place within Lebanese territory.

Article 20 of the same regulation specifies the personal jurisdiction of Lebanese courts as follows: "Lebanese Sharia law shall be applicable to every Lebanese individual, whether they are the perpetrator, instigator, or accomplice, who conducts a felony or misdemeanor outside of Lebanese territory, punishable by Lebanese Sharia law. This provision remains valid even if the individual has obtained Lebanese citizenship after committing the felony or misdemeanor."

The jurisprudence of Lebanon has determined that Lebanon's digital realm on the internet, commonly referred to as "LB," should be regarded as within the confines of Lebanese territory, thereby bringing the Lebanese domain under the purview of Lebanese law.

The Third Chamber of the Criminal Court of Cassation issued Decision No. 175 of 2016, which held: "A social media platform that publishes defamatory expressions is a means of publication designed to inform the public, regardless of whether it is in Lebanon or the Mount Lebanon region, without regard to the plaintiff's place of residence. The Lebanese criminal judiciary has the authority to investigate cases under Article 9 of the Code of Criminal Procedure, and the spatial jurisdiction of the investigating judge in Mount Lebanon is particularly relevant in this instance."

In this situation, the Single Criminal Judge in Keserwan issued Decision No. 927 on November 5, 2011. This ruling was heavily influenced by the computer and its digital information, files, and internet history of the defendant, which were utilized to prove the charges and convict the defendant of creating an electronic account on the website. The plaintiff was targeted with defamatory messages and phone calls for the purpose of discrediting her reputation and dignity. The defendant's defamatory account was found to contain inquiries about the plaintiff's phone number, as well as messages related to the defamation. This account could only be accessed through the defendant's email and password. The criminal judge classified these actions as misdemeanors under Articles 526, 532, and 584 of the Penal Code and imposed financial compensation on the plaintiff in the amount of thirty million Lebanese pounds to address the serious damage to her reputation and dignity, as well as the emotional distress and discomfort caused by her professional position. The judge also ordered Facebook to remove all evidence of the act from the future.

In a ruling issued by the Single Criminal Judge in Beirut, Base No. 164/2012, on February 25, 2020, the defendant was found guilty of disseminating pictures of the plaintiff on Facebook, along with comments and writings that falsely accused the plaintiff of engaging in prostitution and referred to her with derogatory terms, such as "filthy" and other derogatory language. These actions were deemed slanderous and disrespectful, and the defendant was convicted of the misdemeanor outlined in Article 582 of the Penal Code. The defendant was fined two hundred thousand Lebanese pounds as punishment, in accordance with the provisions of Article 582, and this penalty was merged with the

fine stipulated in Article 205 of the same law. As a result, the defendant was required to pay a fine of two hundred thousand Lebanese pounds rather than serving a prison sentence. If the defendant fails to pay this fine, they may be subject to imprisonment for one day for every ten thousand Lebanese pounds owed.

In a ruling issued by the Single Criminal Judge in Case No. 3531/2019 on June 29, 2021, the defendant was found guilty to publish defamatory, slanderous, and insulting messages on her Instagram and Facebook accounts and was convicted of the misdemeanor as per Article 584 of the Penal Code. The court sentenced her to a fine of three hundred thousand Lebanese pounds and imprisonment in the event of nonpayment, as per Article 54 of the Penal Code, with the sentence to be suspended if the fine is paid. The execution of the penalty will be suspended in the event that the defendant pays the fine within three months as compensation for damage caused by the crime, as per Clause (Second) of the ruling within three months of the date of its issuance. The court ordered the defendant to pay the plaintiff an amount of two million Lebanese pounds as compensation for the damage and damage caused to her as a result of the crime. The court further stopped the ongoing tracking of the defendant in accordance with Articles 582 and 532 of the Penal Code due to the inability to track the account on the social media platform Instagram; thus, it was impossible to know the identity of its user, as it was unresponsive.

In a ruling issued by the Single Criminal Judge in Keserwan on July 11, 2023, the defendant was found guilty of the two misdemeanors outlined in Articles 582 and 584 of the Penal Code. The defendant was sentenced to a fine of four hundred thousand Lebanese pounds and imprisonment for one day for each case. Additionally, the court mandated a daily imprisonment sentence of one day for every ten thousand Lebanese pounds of the fine, as per the provisions outlined in Article 54 of the Penal Code in the event of nonpayment and ordered the defendant to compensate the plaintiff with four hundred million Lebanese pounds as reimbursement for damages and losses. The defendant, who is a well-known individual, had posted tweets through his or her Twitter account with the intention of mocking and insulting the plaintiff. These tweets were widely shared and commented upon by the public, and the plaintiff had expressed her opinion on motherhood in a respectful manner through her personal and free opinion without causing any offense to anyone. The defendant was charged with defamation and slander, as outlined in Articles 582 to 586 of the Penal Code, which stipulates that the perpetrator of slander and slander must be punished. The provisions of Article 209 pertain to offenses committed in a public or open space, observed by the public, due to the perpetrator's mistake, or involving words spoken or shouted, verbally or mechanically. Traditionally, such defamation and slander offenses could be committed through deeds, verbal communication, or written communication. However, with the advancement of technology, electronic communication networks have emerged as a new and dangerous means of committing defamation and slander. The informatics industry has created a virtual and intangible space built on electronic digital equations and electrical parts and equipment. Although the Lebanese legislature did not specify automated means, any such means of publication should not be excluded. However, it is not the means of publication but rather the act of publication itself, which constitutes the crime. If a person's communication influences multiple individuals, it may be considered a crime.[18]

[18] It is worth noting that this is a review of some examples of some judicial rulings related to digital violence. The significance of examining judicial rulings related to digital violence cannot be overstated. Therefore, it is imperative to conduct comprehensive research that encompasses judicial cases addressing this issue, particularly given its relevance in formulating appropriate legislation and monitoring requirements.

Role of the Office for Combating Cybercrimes and Intellectual Property[19]

The General Directorate of Internal Security Forces, in accordance with Service Memorandum No. 609/204, 2, dated March 8, 2006, established the Office for Combating Cybercrimes and Intellectual Property. This office is part of the Special Criminal Investigation Department of the Judicial Police in the Internal Security Forces, which is responsible for state security crimes, terrorism, money laundering, and international thefts. The office operates under the supervision of the Public Prosecution of Cassation, the Public Prosecution of Finance, and the Public Prosecution of Appeal in the governorates. It has been granted extensive powers to combat crimes that involve the use of information technologies, including investigating and prosecuting those who commit such crimes. The office is part of the judicial police and is responsible for investigating and prosecuting information crimes in which the advanced technologies used are either the target or the means of committing the crime. Social media crimes fall under the jurisdiction of this office, which conducts the necessary investigation and then refers the case to the public prosecutor to determine whether to pursue prosecution.

The Anti-Cybercrime Office is responsible for a variety of tasks, including combating illegal manufacturing and trade of CDs, safeguarding intellectual and artistic creations, and addressing computer-related crimes such as child trafficking and prostitution. The office also tackles crimes that infringe on public morals, such as those involving the internet, including social media crimes and the spread of viruses. Any comments or responses, including those containing profanity or that violate public morals, that are shared on social media sites are considered crimes and are handled by the Anti-Cybercrime Office, which then refers them to the criminal judicial authorities for further action, including defamation, slander, and contempt. An official source at the Anti-Cybercrime Office emphasized the significance of these efforts in maintaining public order and upholding the law.

The Cybercrime Office initiates investigations in response to either private information or citizen complaints. It also follows the instructions of the competent Public Prosecution to detect, collect, and prosecute the perpetrators of electronic crimes. The office carries out investigations with due speed while preserving the confidentiality of its inquiries into incidents and cybercrimes. Following the completion of its investigations, the office returns the case file to the public prosecutor for a decision on prosecution, and subsequently, the file is transferred to the appropriate criminal authority for further proceedings.

According to a statement from an official source in the Cybercrimes Office during a special interview, the number of complaints related to crimes of digital violence against women increased, especially during the COVID-19 pandemic. The number of reports related to this topic exceeded 750 in 2020 and 2021, and the number of cases reached approximately 1,100 in 2023. Most of the complaints and reports submitted are related to blackmail and electronic threats, and the victims are often women. A statement issued by the General Directorate of Internal Security Forces - Public Relations Division,[20] which states that sexual blackmail complaints received during 2019–2020 to the General Directorate of Internal Security Forces - Public Relations Division - whether via social media or via the "Report" service on its website - show a significant and dangerous increase in numbers. This division received 200 complaints in 2019 and 815 complaints in 2020, an increase of 307.50%.

[19] Review the Internal Security Forces website https://www.isf.gov.lb/ar/cybersecurity

[20] Review the statement on the Internal Security Forces website https://isf.gov.lb/ar/article/9113462

According to the most recent data from Lebanon in 2020,[21] a significant portion of digital blackmail victims were women, accounting for 76% of the total, while 12% were teenagers. In terms of digital violence, some notable incidents include the following:

The family of a minor, who was only sixteen years old at the time, sought the assistance of the security forces after she became the victim of a man in his twenties whom she had met on Facebook. The man had threatened to publish a screenshot of the minor's intimate positions during her conversations if she did not pay him five thousand US dollars. The minor had initially been drawn to the man because of his attractive appearance and had communicated with him daily through the Messenger application, eventually leading to the use of the Video Call feature. Due to the pressures and fear of scandal, the minor approached her father, who subsequently contacted the Public Relations Division of the General Directorate of Internal Security Forces via the "Report" service on their website, filing a complaint against an unknown individual for the crimes of blackmail and threatening his minor daughter by publishing her photos on social media platforms. Following investigations and pursuits, members of the Cybercrime Office were able to identify and arrest the perpetrator, who subsequently confessed to the charges against him and was referred to the Public Prosecution of Appeal.

In this regard, the Cybercrime Office has achieved a notable level of success in processing and addressing a significant volume of complaints and reports related to defamation and digital blackmail. By conducting thorough investigations, the office has been able to uncover the identities of the individuals responsible for these crimes and refer them to the appropriate judicial authorities. The following are some examples:

- On December 26, 2023, the Anti-Cybercrime Bureau,[22] aided by the judicial police, apprehended several individuals on charges of stalking, financial blackmail, defamation, and group defamation. These individuals threatened to disseminate the photographs or phone conversations of a group of female citizens and posted defamatory content on social media.
- On January 9, 2021, two individuals were charged with taking photographs of a minor female[23] to obtain money from her by deceiving her to hack the second individual's phone and deleting her images from it. They were also charged with attempting to harass the victim because they had an emotional relationship with her. Following their arrest, the Cybercrime Office deleted the images from one of the suspect's phones and transferred them to the appropriate authority in accordance with a judicial order.
- On August 8, 2021, a suspect was apprehended and charged with fraud to create multiple fake accounts using pictures of foreign models with Lebanese names and video clips, with the intent of deceiving individuals into dating and meeting them to obtain "cell phone charging cards."
- On July 9, 2023, a person was apprehended and charged with disseminating pictures and defamation. Following his admission to being involved in a relationship with the plaintiff, he allegedly sent him intimate photos due to pressure. When she asked him to end the relationship, he published her photos with the intention of defaming her after she asked him to end their relationship. The defendant's phone was confiscated, and he was taken into custody to face charges in court in the appropriate judicial authority.[24]

---

[21] An increase in the number of electronic blackmail crimes: Security forces are on the lookout and associations follow up on the rehabilitation of victims, 2022, Hassan Haider. Increase in the number of cyber-extortion crimes by security forces https://www.elnashra.com/news/show/1576359/

[22] To review the report issued by the General Directorate of Internal Security Forces- Public Relations Division https://www.isf.gov.lb/ar/article/9116341

[23] To review the report issued by the General Directorate of Internal Security Forces- Public Relations Division https://isf.gov.lb/ar/article/9113352

[24] This news was published on the website Security and Judiciary/638159 https://www.nna-leb.gov.lb/ar/

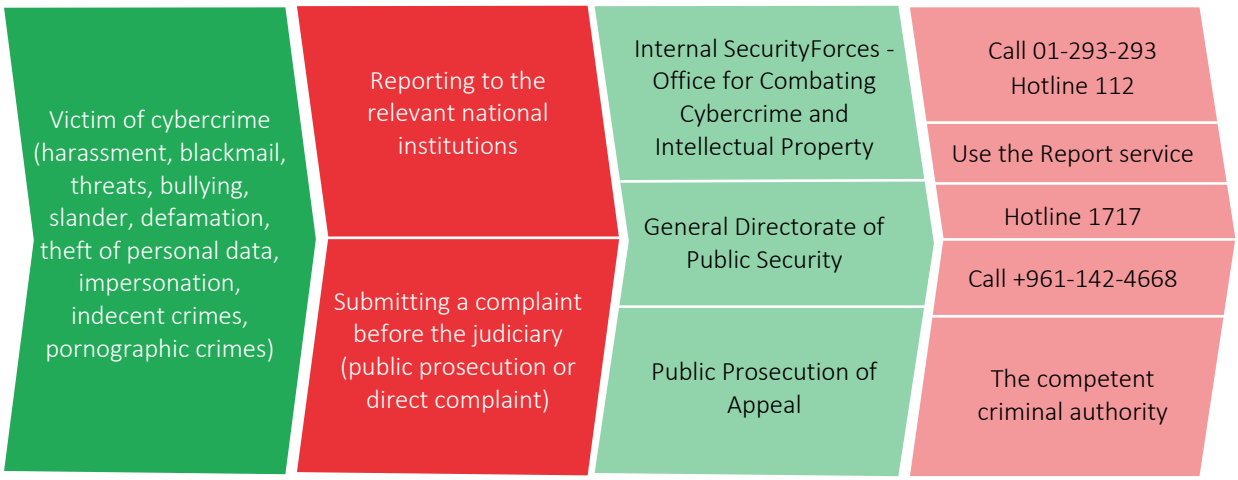
- On June 16, 2021, a suspect was taken into custody for allegedly threatening and blackmailing a citizen, demanding that she send intimate photos and videos and subsequently use her account to implicate other individuals. Reportedly, the individual compromised over 750 accounts across Facebook and Instagram applications. The case was referred to the appropriate court for further proceedings.[25]

The Internal Security Forces at the General Directorate undertake awareness-raising initiatives to educate the public about cyber risks and preventative measures against cybercrimes. By providing guidelines and resources on their website and social media platforms, they aim to raise awareness about electronic blackmail, the protection of families and children, and the safeguarding of electronic devices. The directorate also advises citizens on appropriate online behavior, warning them against falling prey to blackmail, indecent, or exploitative acts, and cautioning against communicating with unknown individuals on social media platforms. In the event of such incidents, individuals are encouraged to contact the General Directorate of Internal Security Forces, specifically the Office for Combating Cybercrimes and Intellectual Property, or to report the matter to the relevant judicial authority[26] (see Appendix No. 1 - Information Security and Risk Awareness Guide issued by the General Directorate of Lebanese Public Security).

Subsequently, the General Directorate of the Internal Security Forces made several avenues available for citizens to report instances of blackmail, electronic defamation, or any form of electronic crime. The following options are available for reporting instances of blackmail or electronic bullying:

- Report to the Internal Security Forces any attempts of blackmail or digital bullying by calling the Internal Security Forces hotline at 112.
- Use the "Report" service on the Internal Security Forces website (isf.gov.lb) by filling out an electronic form or sending an email to ballegh@isf.gov.lb (see Attachment No. 2 - the notification form on the Internal Security Forces website).
- Contact the Office for Combating Cybercrimes and Intellectual Property at 01/293293.
- Contact the General Directorate of Lebanese General Security at 1717 within Lebanon or 009611424668 from outside Lebanon, or through the social media account of General Security (Facebook account of General Lebanese Security - General Directorate of Lebanese General Security) or (X @DGSG_Security).

Means of reporting a cybercrime incident



[25] This news was published on the website https://www.zamanalwsl.net/news/article/138019/

[26] To review the information security and risk awareness guide issued by the General Directorate of Lebanese Public Security and published on the website: https://www.general-security.gov.lb/uploads/cyber_awarness_booklet.pdf

Role of National Public Institutions in Providing Protection in Cases of Digital Violence Against Women

1. Ministry of Social Affairs[27]

The Ministry of Social Affairs, in alignment with contemporary notions of human development and social responsibility, incorporates a social work strategy that aims to safeguard and assist marginalized groups, notably women, minors, and children who have fallen victim to gender-based violence. In 2020, the Ministry unveiled its strategic plan for the protection of women and children, which will be in effect from 2020 to 2027.[28] This plan was devised in partnership with UNICEF and the European Union, and its primary objectives include bolstering the ministry's leadership and regulatory role in child protection and combating gender-based violence. This strategy emphasizes the importance of fostering coordination and integration between the public and private sectors, as well as civil society, to ensure that comprehensive and high-quality services are available to the target population. This approach aims to strengthen the national system and address child protection violations and gender-based violence. Since 2014, the ministry has been implementing the National Strategy for the Protection of Children and Women, which has resulted in significant progress in the ministry's efforts to protect children. In 2015, the ministry achieved a milestone by establishing and implementing unified executive procedures for child protection.

Mrs. Claudine Aoun Roukoz, the President of the National Commission for Lebanese Women, emphasized the need for coordinated efforts between official institutions to implement strategies for the protection of women and children during the launch ceremony of the strategic plan for the period 2020-2027. She also emphasized the importance of approving laws that recognize women as citizens with full rights. Additionally, Mrs. Aoun highlighted the critical role of social development centers in responding to the needs of marginalized groups, particularly women and children, and called for increased support and activation of these centers to provide essential services to these groups.[29]

The Ministry of Social Affairs offers a range of services to survivors of gender-based violence via a network of secure facilities that were established in accordance with the "Strategic Plan for the Protection of Women and Children in Lebanon 2020-2027." The plan encompasses a variety of initiatives. The following are the most significant ones:

1. Psychosocial Support: Available at several development centers affiliated with the ministry, this service provides follow-up and support to women and children in overcoming the effects of the past and developing their personal abilities. The goal is to reintegrate them into their families and society.
2. Legal Consultation: Aimed at raising women's awareness of their rights and duties, this service offers legal advice and follow-up in both religious and civil courts.

[27] Check the website of the Ministry of Social Affairs https://www.socialaffairs.gov.lb/

[28] To learn more about the “Strategic Plan for the Protection of Women and Children in Lebanon 2020-2027” https://www.unicef.org/lebanon/ar The Ministry of Social Affairs launches the extended-strategic plan for the protection of women and children from/Press releases.

[29] To learn more, please see: https://nclw.gov.lb/4130/Claudine-Aoun-Roukz-at-the-launching-ceremony-of-the-plan/

3. Sociocultural Support: This service focuses on enhancing women's self-confidence by introducing them to their rights and helping them develop their abilities. Additionally, this service attempts to improve family and social relations through awareness and education on positive parenting, responsibility, and communication skills. It also covers childbirth preparation and infant care, as well as organizing various recreational programs and activities.
4. Vocational Rehabilitation: This service aims to empower women professionally and provide them with life skills training to help them become self-sufficient. It also supports women in engaging in the labor market.

In addition to offering various services, including providing internal or external care, healthcare through a gynecologist, and a nursery for childcare, our organization is committed to supporting early childhood and working women. To this end, mechanisms have been created to promote their participation in the labor market, enhance their psychological and social stability, and improve their self-esteem. This positive impact is reflected in their economic, family, and job stability, as well as their performance and contribution to increasing their productivity. Furthermore, craft courses, such as sewing, embroidery, and soap manufacturing, are provided to further empower and equip our clients with valuable skills.

In 2023, the Ministry of Social Affairs and the "Abaad" organization jointly released the "National Standard Operating Procedures for Cases of Social Role-Based Violence" document.[30] This document aims to establish a clear and unified framework by defining roles and providing concrete tools to organize common interventions among all relevant official sectors, including the Ministry of Justice, the Ministry of Health, the Ministry of Interior and Municipalities, and the Ministry of Social Affairs, as well as concerned civil organizations. This document is intended to enable protective humanitarian actors to implement necessary measures, such as adhering to minimum standards of prevention and responding to various situations of violence at all stages of crises and stability.

The Ministry of Social Affairs also plays a leadership and regulatory role in protecting children at risk in accordance with the Convention on the Rights of the Child, which Lebanon has ratified and is committed to implementing its provisions under Law No. 422 of 2002, the Law for the Protection of Juveniles in Conflict with the Law or at Risk.

The Ministry of Social Affairs takes action based on the following:

- The information provided includes alarming data on severe forms of abuse, neglect, exploitation, and violence that negatively impact a child's development, life, health, and dignity, hindering their growth and progress.
- A complaint is received from the affected individual through the "Send a Complaint"[31] service available on the ministry's website.
- Contact the ministry's central number at +961 1 611 260/4 or reach out to the ministry's distributed centers throughout various regions in Lebanon.[32]
- Contact the ministry's employees via the Facebook application on the ministry's website.
- Send an email to the address info@socialaffairs.gov.lb.

[30] To learn more about this document, please review the website: https://www.socialaffairs.gov.lb/news/

[31] Form for sending a complaint to the Ministry of Social Affairs https://www.socialaffairs.gov.lb/complaint

[32] Means of contacting the centers of the Ministry of Social Affairs: https://www.socialaffairs.gov.lb/our-centers

2. Ministry of Education and Higher Education[33]

Within the context of creating a secure and nurturing environment for both male and female adolescents, the Ministry of Education has actively taken steps to guarantee a conducive atmosphere for quality and equitable education. It has placed the welfare of children and teenagers and their optimal conditions at the forefront of educational priorities and commitments. In response to Lebanon's dedication to achieving its Sustainable Development Goals (2015-2030), the ministry strives to foster the growth and development of children by addressing their mental, cognitive, social, and emotional needs in a safe and secure environment. Since 2012, the ministry has implemented the preventive program PROTECTED to safeguard children from sexual harassment in educational curricula. This initiative helps to protect children and instills a sense of self-respect and regard for others. Additionally, the ministry has organized educational workshops on protecting children from harassment and violence.[34] In 2018, the Ministry of Education launched the Student Protection Policy in the School Environment as part of a broader program aimed at ensuring quality and flexible education for all. The ministry has provided students with:

- The hotline service 01772000, which is operational 24/7, has been established to receive any and all complaints pertaining to instances of violence. Upon receiving notification of any such complaint, the Ministry of Education refers the matter to the appropriate judicial authority.
- The ministry has established a department dedicated to child protection and school integration that offers psychological and social support and collaborates with the security forces and the Ministry of Justice to ensure the safety of female students through the guidance system.

The Ministry of Education and Higher Education, in collaboration with the National Authority for Women and UNICEF, recently launched a series of tours targeting secondary schools with the aim of raising awareness about violence prevention for girls. During the launch, the Minister of Education emphasized the ministry's unwavering commitment to combating any form of harassment or discrimination against girls and reassured the public that it is fully prepared to address any suspicious situations that girls may encounter.

3. National Commission for Lebanese Women (NCLW)[35]

The National Commission for Lebanese Women was formed in accordance with Law No. 720, which was enacted on November 5, 1998. This official organization reports to the Presidency of the Council of Ministers and aims to further the rights and interests of women in Lebanon. The law mandates that the National Authority provide advice to the government and other public bodies on matters related to women and gender issues, coordinate efforts among public institutions and nongovernmental organizations working on gender issues and carry out executive tasks such as developing national plans and strategies to support women's progress and implementing projects aimed at improving women's conditions.

The Executive Director of the National Commission for Women's Affairs, Ms. Micheline Massad, emphasized that the National Commission is associated with the Presidency of the Council of Ministers and operates at the national level by implementing strategies, action plans, and projects. Additionally, she highlighted that psychological follow-up for victims is conducted by civil society organizations and

[33] Review the website of the Ministry of Education and Higher Education https://www.mehe.gov.lb

[34] Launching a preventive program to protect children from sexual harassment, including it in educational curricula, and funding from the Bank of Lebanon Migration https://www.annahar.com/arabic/article/6666-

[35] Review the website of the "National Commission for Lebanese Women" https://nclw.gov.lb/

that the commission is fully committed to coordinating closely with these organizations and the General Directorate of Internal Security Forces.

Within this context, the National Authority for Women's Affairs, in collaboration with its public and civil sector partners, developed the "National Strategy for Women in Lebanon 2022-2030. "[36] This strategy outlines five primary objectives based on the vision that "women in Lebanon hold leadership positions in all fields and are equal to men in terms of rights and obligations in a state governed by the rule of law and where human rights are protected." The preparation of this strategy was prompted by efforts to achieve sustainable development goals by 2030 and the Lebanese government's adoption of a national plan to implement Security Council Resolution 1325 on women, peace, and security in September 2019. Additionally, the International Committee on the Implementation of the Convention on the Elimination of All Forms of Discrimination against Women issued concluding observations. This strategy seeks to attain dynamic gender equality by providing women and men with equal opportunities in directing their life courses, personal lives, and the choices of the society in which they reside. In other words, the law governing the public must guarantee these rights, and the institutions must protect and observe the law. Among the five main objectives outlined in this strategy, the first goal is to combat violence against women in all its forms.

Accordingly, the Minister of State for Women's Affairs established the "National Strategy to Combat Violence against Women and Girls in Lebanon 2019-2029." This strategy's primary objective is to prevent and safeguard women from gender-based violence. Such violence encompasses domestic violence, including economic, psychological, emotional, physical, and sexual abuse, as well as physical assault, harassment, and rape. Additionally, it covers forced and child marriages, online violence or electronic blackmail, human trafficking, and forced prostitution.[37]

To attain the primary objective, the National Commission for Women's Affairs delineated three subgoals:

1. The first subgoal entailed broadening knowledge regarding the incidence of violence and the prevalence of acts of violence against women.
2. The second subgoal entailed implementing extensive measures to preclude the spread of violence against women and safeguard them.
3. The third subgoal involved ensuring access to justice and providing support to victims.

Prominent among the preventive measures outlined in this strategy is the empowerment of women through education, scientific, and technical means, as well as the dissemination of awareness about the potential dangers associated with the use of the internet and social media. Additionally, this strategy emphasizes educating women about the risks of digital blackmail and sexual harassment, as well as providing guidance on seeking assistance from educational institutions and services provided by the Ministry of Education and higher education and security services. Furthermore, the strategy proposes the enactment of a legislative policy that includes positive discrimination measures in favor of women. This policy includes the adoption of a law that safeguards politically active women, particularly women candidates for political office, from violence, threats of violence, or defamation campaigns, including those conducted through electronic media.

---

[36] Members of the Arab Center for the Development of the Rule of Law and Integrity participated in the meetings to prepare the national strategy for women in Lebanon 2022-2030, and they enriched the text of this strategy with their observations and comments in cooperation with other organizations from civil society.

[37] To review a report on the implementation process of the "National Strategy Action Plan to Combat Violence against Women and Girls 2019-2029" https://nclw.gov.lb/wp-content/uploads/2022/06/NCLW-VAWG-Stocktaking-Strategy.pdf

The National Commission for Lebanese Women recently announced the outcomes of public opinion polls conducted in Lebanon between 2021 and 2022 pertaining to "Violence against women, blackmail, digital harassment, and sexual harassment." This falls within the gender equality barometer for Lebanon, which is a part of the project "Combat violence against women in Lebanon and prevent it from occurring," implemented by the National Authority in collaboration with the GIZ. This project is funded by the German government as a part of a larger program.[38]

The findings of these surveys, which were carried out on a sample of 250 women divided into six age categories ranging from eight to fifty years old, indicate that 20% of the participants had experienced digital blackmail, while 80% had not. Additionally, 10% of the participants had encountered a digital threat, while 90% had not. These threats were primarily carried out through social media platforms, particularly Facebook, Instagram, and WhatsApp. The survey results revealed that only 31% of the women who experienced digital threats and blackmail reported incidents. A significant majority of the participants (89%) had positive knowledge and awareness of digital blackmail, while 86% were aware of digital harassment. However, it is important to note that some participants had not been exposed to such incidents.

In 2022, the National Commission for Lebanese Women, in conjunction with the Ministry of Education and Higher Education and in collaboration with UNICEF, initiated a series of school tours to several public high schools as part of the "Empowered and Capable Girls: Education for All" project. This project aimed to provide awareness sessions targeting 3,000 female students and equipping them with essential supplies, particularly those that promote the protection of girls (LAHA KIT).[39]

Mrs. Claudine Aoun Roukoz, the President of the National Commission for Lebanese Women, stated during her recent tours, "To combat the violence that one may encounter in their home or academic environment, it is essential to disclose it and seek assistance through the Ministry of Education's hotline at 01772000."

4. Telecommunications Regulatory Authority[40]

The establishment of the Telecommunications Regulatory Authority was mandated by Law No. 431, which was issued in 2002. This government agency is responsible for the regulation and development of the telecommunications sector in Lebanon. Its mission includes the liberalization of the industry, the issuance of licenses and regulations, and the management of frequencies and communications. The authority is also responsible for granting licenses to technical service providers, which facilitates the process of obtaining digital evidence related to the movement of communications and digital data.

The responsibilities of this regulatory body include the maintenance of cybersecurity. To fulfill its mission of safeguarding the rights of telecommunications consumers, numerous measures have been taken to protect minors on the internet. These include providing informative resources for parents on their website,[41] along with monitoring tools to help parents keep their children safe online.

[38]- To review the opinion poll study on: “Violence against women and girls, blackmail, electronic harassment, and sexual harassment,” see: https://nclw.gov.lb/wp-content/uploads/2023/03/LGEB_Cyber-Extortion-and-Cyber-Harassment.pdf

[39] To review the website of the National Authority for Women’s Affairs https://nclw.gov.lb/5630

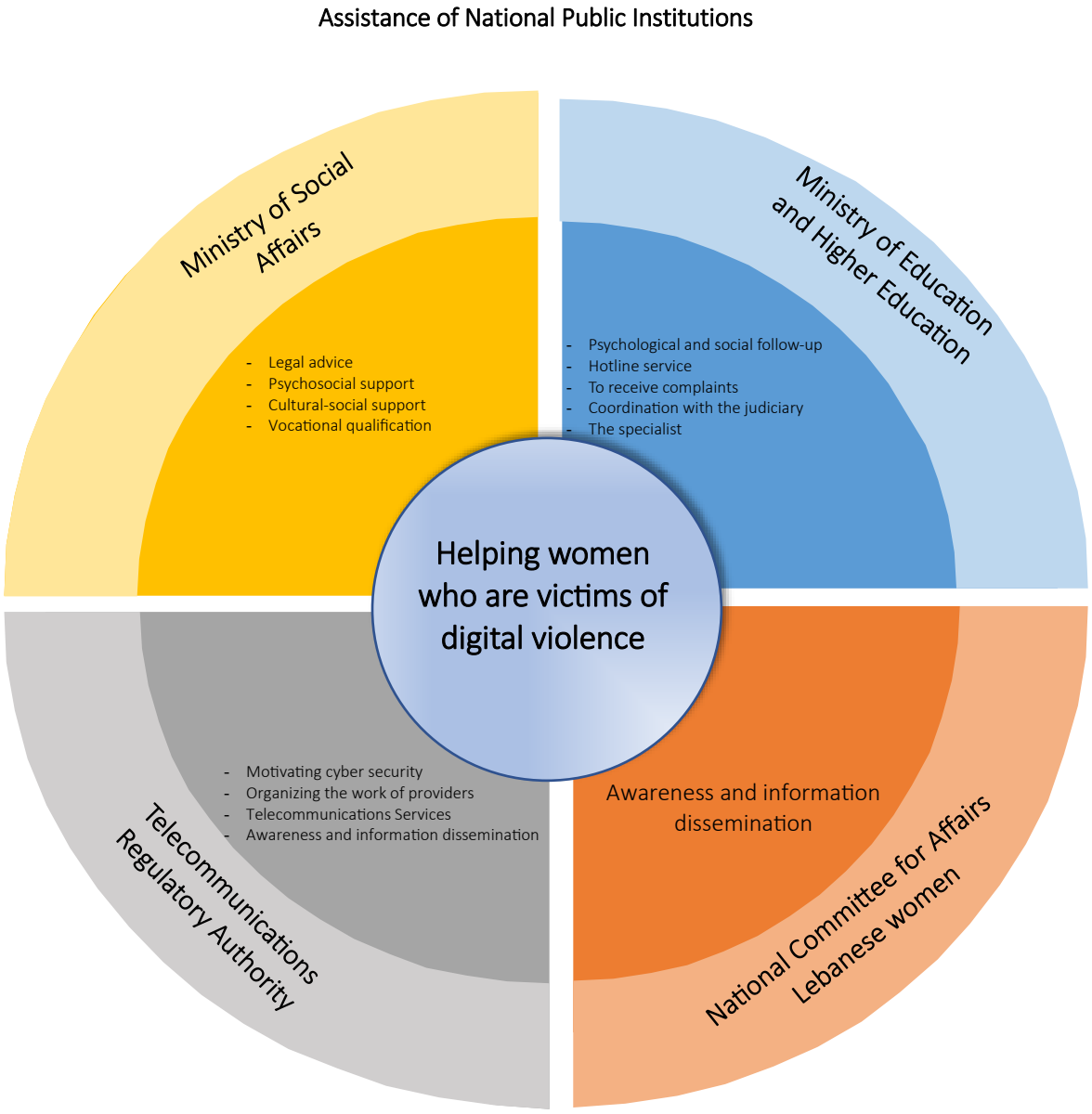
[40] Check the Telecommunications Regulatory Authority’s website http://www.tra.gov.lb/

[41] Review the Telecommunications Regulatory Authority’s website- Child Protection http://www.tra.gov.lb/children-protection-AR

The regulatory authority has formulated a comprehensive strategy and vision that encompasses a range of regulatory initiatives aimed at fostering cybersecurity. The following are the main ones:

1. Develop a draft on cybersecurity and child online protection that can be adapted and utilized in ways consistent with national laws and norms.
2. Encourage those concerned with stimulating the adoption and implementation of policies and strategies that protect cyberspace and children in cyberspace and promote safer access to the exceptional opportunities provided by internet resources.
3. Issue a set of recommendations and regulations for communications service providers to ensure information security in communications infrastructure and establish conditions for service providers requiring them to adhere to network protection and service security standards, such as ISO 27, and maintain public safety. This forms part of comprehensive systems governing the collection, use, and dissemination of information and data.
4. Update the consumer affairs system to include cybersecurity requirements.
5. Prepare regulations specific to the sector that include conditions that take into account the laws of commerce, electronic services, and cyberspace protection.

The authority is taking steps to create a Computer Emergency Response Center to mitigate and prevent significant incidents, as well as safeguard its valuable assets. This center serves as a central coordination point for IT security issues in the country and employs specialized experts to address and respond to IT incidents. The center's primary responsibility is to assist and support users in quickly recovering from security incidents, and it also handles legal issues, preserves evidence for potential lawsuits, fosters cooperation within the IT Security Department by promoting awareness, and monitors advancements in the field of IT Security.


Assistance of National Public Institutions
Ministry of Social Affairs
- Legal advice
- Psychosocial support
- Cultural-social support
- Vocational qualification
Ministry of Education and Higher Education
- Psychological and social follow-up
- Hotline service
- To receive complaints
- Coordination with the judiciary
- The specialist
Helping women who are victims of digital violence
Telecommunications Regulatory Authority
- Motivating cyber security
- Organizing the work of providers
- Telecommunications Services
- Awareness and information dissemination
National Committee for Affairs Lebanese women
Awareness and information dissemination

Role of Civil Society

Civil society plays a crucial role in safeguarding women from digital violence. It considerably contributes to raising awareness and disseminating information about digital violence, its various forms, and digital protective measures. By providing free legal assistance through the HelpDesk service and psychosocial support centers for women who have experienced digital violence, civil society organizations can provide essential legal and psychological support. Additionally, these organizations work toward enhancing legislation that protects women from digital violence and ensures its effective implementation by authorities. They achieve this by conducting campaigns and social activities that put pressure on governments to combat digital violence and promote societal rejection of harmful behaviors. Civil society organizations also influence public opinion, change prevailing masculine practices, mentalities, and concepts, and demonstrate solidarity with victims of digital violence. Moreover, they contribute to developing effective strategies and policies by monitoring and collecting data on digital violence cases, documenting them, and publishing reports and research that highlight the extent of the problem and the challenges that women face in this context. Overall, civil society can be a valuable partner in combating digital violence and protecting women's rights by monitoring needs, providing support, empowering women who are victims of violence, and advocating for improved legal and social environments that ensure women's rights and digital security.

The movements of women's civic organizations in Lebanon have played a crucial role in promoting women's rights and combating gender discrimination and sexual and digital violence against women. Recently, advocacy and awareness campaigns have been launched in Lebanon to combat violence against women in all its forms and types, with the aim of raising awareness about the negative consequences of such violence. To address the root causes of this problem, it is necessary to change discriminatory social norms and gender stereotypes and involve the entire community in the process. Additionally, empowering women in the economic, political, and social fields can help enhance their resources and skills, improve access to justice for survivors of violence, and end impunity for perpetrators of violence against women.

In this vein, certain women's organizations have taken to provide legal and psychosocial aid to support and facilitate the recovery and reintegration of victims of digital violence into society. This study highlights the foremost nongovernmental organizations that strive to combat gender-based violence and the available means for reporting instances of violence against women. Illustrative examples include but are not limited to the following:

1. Women's Committee of the Beirut Bar Association[42]

The Women's Committee of the Bar Association is committed to advancing women's roles in social development and public life. This is achieved by promoting the idea that "no social development can occur without complete equality between the sexes and the eradication of all forms of discrimination, and no sustainable development can be attained without an active role for women as essential agents of change." To this end, the Women's Committee works to raise awareness about achieving equal rights between men and women, combating gender-based violence, fostering collaboration with international, regional, and national organizations, and unifying efforts to enhance the constructive role

[42] Refer to the Beirut Bar Association website https://bba.org.lb/

of women in society. Additionally, the committee is dedicated to providing necessary protections for women and combating violence in all its forms.

Ms. Asma Hamadeh, the Chair of the Women's Committee of the Beirut Bar Association, remarked in a recent interview, "The frequency of incidents involving digital violence against women, particularly adolescent girls between the ages of sixteen and twenty-five, has risen significantly in the absence of an effective mechanism for addressing these crimes. It is crucial to establish a system for monitoring and holding perpetrators accountable for crimes of digital violence, particularly those involving digital blackmail targeting women, who may be subjected to the manipulation of their photos or other harmful methods." Ms. Hamadeh emphasized "the need for strict enforcement of the law and severe penalties for perpetrators, without showing leniency in such cases, as is currently the practice. In many instances, the perpetrator is merely required to sign a pledge not to commit further offenses without facing any significant consequences."

Ms. Hamada indicated that the Women's Committee of the Bar Association actively engages in combating digital violence against women through the organization of lectures, workshops, and awareness campaigns on this topic. However, it is important to note that the committee does not possess a hotline to offer direct legal advice, as is often the case with nongovernmental organizations.

Ms. Hamada emphasized the need for comprehensive safeguards to protect women subjected to digital violence through three primary recommendations: 1) implementing an efficient monitoring mechanism to hold perpetrators of digital violence accountable and imposing stringent penalties to deter the spread of such crimes; 2) enacting strict laws to curb the proliferation of digital blackmail and other violence offenses; and 3) launching extensive awareness campaigns to combat digital violence against women, with a focus on targeting female students at schools and universities.

2. "Enough Violence and Exploitation" Organization (Kafa)[43]

Kafa is a nongovernmental, civil, and nonprofit organization located in Lebanon that aims to eliminate discriminatory and patriarchal structures that exist toward women in the areas of social, economic, and legal systems. Since its inception in 2005, Kafa has been working to eliminate all forms of gender-based violence and exploitation and to achieve true equality between men and women. To achieve this goal, Kafa employs various methods, such as advocating for the introduction and amendment of laws and policies, changing prevailing patriarchal attitudes, practices, and concepts that are harmful to women, conducting research and training, empowering women who have experienced violence, and providing them with protection, psychological, social, and legal support. In this regard, Kafa provides the following aid to victims of gender-based violence, including those who experience digital violence:

- Legal and psychosocial assistance may be obtained by calling the organization's offices at 96101392220 or via email at kaf@kafa.org.lb.
- A hotline call service is available at 1745.
- A support line service is offered to obtain free assistance by calling 96103018019—available 24/7. Notable services provided by the Support Center for women who are victims of violence include:
    - Social intervention by a social worker is implemented to identify issues and create tailored action plans for each woman.
    - Psychological assessments conducted by psychologists and subsequent referrals to psychological treatment, when necessary, are also provided.

[43] Refer to the KAFA organization's website https://kafa.org.lb

- Legal advice and dedicated support throughout the appropriate legal processes are available for each woman.
- Referrals to safe centers are made.
- Forensic doctor's reports documenting incidents of violence are also supplied to the victim to provide necessary documentation.

3. ABAAD Organization[44]

The Resource Center for Gender Equality (ABAAD) is an organization that has been accredited by the United Nations Economic and Social Council, with the goal of promoting gender equality as a fundamental condition for sustainable social and economic development in the Middle East and North Africa region. As the copartner of the National Technical Task Force to End Gender-Based Violence against Women (alongside the Lebanese Ministry of Social Affairs), ABAAD has been working toward developing and implementing policies and laws that promote the active participation of women since 2012. The organization also supports and builds the capacities of local, regional, and international entities that work in protection programs, case management, sexual and reproductive health and rights (SRHR), mental health, psychosocial support, and gender. In addition, ABAAD aims to effectively involve men in working toward a just society that is free of hegemonic masculinity and violence against women.

To eradicate gender-based violence, ABAAD employs a comprehensive care strategy that provides protection and support services to survivors of such violence/rights holders in both peaceful and turbulent times, as well as during disasters. This is facilitated by offering the following:

- Al Dar Al Amn Center (Safe House) for Women is a secure and temporary facility that provides refuge to women who are exposed to or at risk of violence. The center offers a range of services, including psychosocial support and mental health services, legal advice, social guidance services, socioeconomic empowerment activities, social health awareness and education, and life skills training. The center also provides an emergency safe line (+9618-178-8178), which is available 24/7, as well as a secure line (+9617-606-0602), via email at the following address: accountability@abaadmena.org, and a secure WhatsApp communication channel through the organization website.

4. FEMALE Organization[45]

FEMALE is a nonprofit, community-based feminist organization that aims to create a just and safe world for women in all their diversity by driving social behavioral change, building movements, producing, and disseminating knowledge, and advocating for policy reform. The organization has four centers in remote and marginalized areas, including Tripoli, Nabatiyeh, Beirut, and Beqaa. These centers provide a safe space for women, nonbinary individuals, and marginalized youth to connect, express themselves, share ideas, learn, develop their skills, and access resources.

The FEMALE organization additionally offers legal and social psychological assistance services. These services are accessible through:

- The provision of a support and assistance line at 96181111456
- A digital safety and security guide specifically tailored for teenage girls in Lebanon.[46]
- An introductory book aimed at identifying and preventing digital violence against women.

[44] To refer to the website of the Abaad Organization https://www.abaadmena.org/

[45] To refer to the website of the FEMALE organization https://www.fe-male.org/

[46] To review the guide to digital safety and security for teenage girls in Lebanon: www.instagram.com/femalecomms/p/C2uaCk8IU4k/?img_index=1

In collaborating with ActionAid, FEMALE initiated the "National Network to Challenge the Depiction of Women in Media and Advertising in Lebanon" initiative. This ongoing effort aims to illuminate all forms of gender discrimination propagated by the media and advertising to viewers and consumers and to apply pressure and raise awareness about this issue throughout Lebanon.

In Lebanon, FEMALE launched a campaign to raise awareness about digital violence against women under the title "The Screen Does Not Protect." This campaign emphasized that women in Lebanon and the Arab world have the right to access and use the internet freely and safely without being subjected to electronic violence. The objective of the campaign was to educate women about their rights to use the internet and the various threats and challenges associated with it, as well as to provide them with safe usage techniques, particularly on social networking sites. The campaign also aimed to inform women and girls that they can hold the aggressors accountable for their actions, even if the assault took place on social media sites, by reporting and exposing them.

In an exclusive interview, Ms. Hayat Murshad, the founder of the FEMALE organization, stated that FEMALE has been addressing the issue of digital violence since 2020. This was due to the increase in reported cases of digital violence following the outbreak of the COVID-19 pandemic, which brought increased attention to this type of violence. According to official statistics, women and girls between the ages of 13 and 21 are particularly vulnerable to such cases. The use of digital technology to perpetuate violence against women is a disturbing trend that has recently emerged. This form of violence encompasses various types of harassment, such as digital harassment and blackmail, theft of personal information and accounts, and the sharing of private details. These heinous acts have far-reaching psychological and social consequences for victims, particularly when they are subjected to blackmail. The lack of knowledge and resources to protect themselves, coupled with the fear of stigma and shame, often leads to submission to the demands of the perpetrator. It is essential to recognize the severity of this issue and take appropriate measures to mitigate its impact.

> Digital violence, when it transpires in the virtual world instead of the physical world, must not be dismissed as insignificant. In fact, it can have detrimental consequences for women and girls. Unfortunately, we have recently witnessed several instances of young women and adolescents taking their own lives as a result of digital violence and coercion.

According to the organization, several recommendations are critical for addressing the issue of digital violence. These include 1) intensifying and expanding awareness campaigns to educate individuals about digital protection mechanisms and the various methods and means used to perpetrate digital violence; 2) imposing strict penalties and expeditiously responding to reports of digital violence while maintaining confidentiality to protect the privacy of victims; 3) encouraging collaboration among civil society organizations, judicial and security institutions, and various sectors to address the issue; 4) emphasizing the importance of schools and parents in supporting teenage girls and addressing digital violence, with a particular emphasis on the role of the Ministry of Education in providing a reporting mechanism for such incidents; and 5) advocating for the establishment of a specific law for digital violence and blackmail to address the growing prevalence of this phenomenon.

5. "Himaya" Organization[47]

Himaya, established in 2008, is a nongovernmental organization specializing in the child protection sector. It focuses on preventing violence against children and offering support at the psychological, social, and legal levels to abused children, thereby enabling their reintegration as productive and active members of society. In 2018, Himaya became a member of the International Social Service (ISS), which addresses cases of cross-border child abuse involving a Lebanese and foreign parent. Additionally, Himaya has been authorized by the Ministry of Justice to handle all legal protection issues in the North Governorate.

Himaya also provides legal and social psychological support through various means, including:

- The Hemaya electronic helpline[48] aims to provide a secure online environment for children and young adults. This service offers technical support for internet safety, legal guidance for cybercrime or cyberbullying, an avenue for voicing worries, posing inquiries, and reporting abuse.
- The helpline can be accessed by calling 0341-496-4961.

6. Lebanese Women Democratic Gathering (RDFL)[49]

The Lebanese Women Democratic Gathering (RDFL) is a secular nongovernmental women's organization that was established in 1976 to advocate for the rights of women in Lebanon. As one of the oldest women's organizations based on volunteer work, gatherings are committed to achieving full equality between women and men in all fields and ensuring protection from gender-based violence. To raise awareness among society, particularly women, about their rights, the Lebanese Women Democratic Gathering has implemented several projects and campaigns. One of its most prominent campaigns is #Your Security-Your Protection-Priority, which encourages women to report any type of violence they experienced during the lockdown as a result of the COVID-19 pandemic.

The campaign was an electronic march that was shared with a large number of influencers in Lebanon to establish effective safeguarding measures and encourage the reporting of gender-based violence and sexual and gender-based violence in Lebanon. This initiative sought to empower women and girls who had experienced violence by equipping them with the necessary tools for protection through the following:

- Report any instances of violence by calling the hotline service at 71500808, which is available 24/7 and offers a confidential and complimentary service.
- This service also provides support for psychological, social, and legal matters.

On the other hand, nongovernmental organizations are striving to establish digital platforms to promote women's rights and empower them through awareness campaigns. Some of these platforms include:

- The "Partner But"[50] platform is an independent feminist news website that serves as an extension of FEMAIL's mission to raise awareness and advocate for women's issues in Lebanon, the Arab world, and the world at large. This is achieved through its initial initiative, which is the first feminist radio program of its kind in Lebanon and the Arab world. The platform aims to monitor the situation of women in Lebanon and the Arab world and to disseminate related news on a wide legal and media scale.

[47] To review the website of the "Himaya" organization https://www.himaya.org/

[48] The e-helpline is available at https://www.himaya.org/content/learn-more-about-e-helpline-1

[49] To review the website of the Lebanese Democratic Women's Gathering https://www.rdflwomen.org

[50] To review the website of the "Shareka But" platform https://www.sharikawalaken.media/

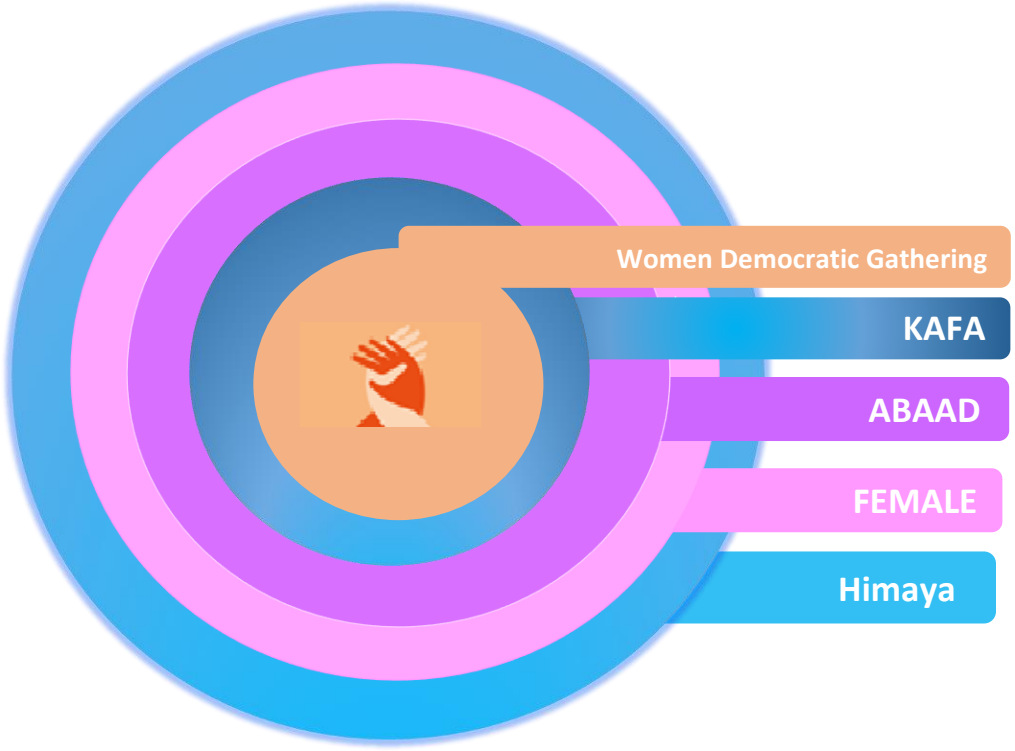
Additionally, this platform supports the work and struggles of women's and human rights organizations in Lebanon and the Arab world by relying on sound and reliable sources, impartiality, transparency, objectivity, and nondiscrimination. The platform strictly adheres to these principles and refrains from broadcasting any content that promotes violence, sectarianism, racism, intolerance, or discrimination.

- The "Fifty-Fifty" platform[51] is a nongovernmental organization based in Lebanon that seeks to promote gender equality in both the public and private sectors, with a particular emphasis on political decision-making positions. It works to combat digital violence against women who participate in political life by lobbying stakeholders to reform gender laws and establishing a think tank composed of experts who specialize in developing ongoing strategies. Additionally, it partners with the media to showcase the achievements of prominent women on an equal basis with their male counterparts. The organization's efforts are focused on promoting gender equality and empowering women in all aspects of society.
- The Khateera platform, dubbed 'Dangerous,'[52], is a women-led media platform in Beirut that focuses on women with diverse backgrounds and challenges in the Middle East and North Africa. Its initiatives seek to unveil biases, prejudices, and stereotypes directed at women, as well as factors impeding their equality with men. The organization offers a secure space for discussing feminism, patriarchy, and sensitive social issues in an accessible and uncomplicated manner.

[51] To review the Fifty-Fifty organization's website www.fiftyfiftylb.com

[52] To review the website of the "Khateera" platform https://khateera.com/

Civil Society Organizations Providing Legal, Psychological, and Social Support



Non-Governmental Organizations Providing Aid to Victims of Violence

Providing immediate assistance

- Report any case of violence via the hotline service, which is available 24/7, while maintaining the confidentiality and freeness of the service.
- Contact the organization's security line or communicate via WhatsApp.
- Sending an email to the organization.

Providing legal, psychological, and social support

- It provides counseling and psychological services to help victims deal with the effects of digital violence on their psychological and social health.
- Providing legal support to victims by guiding them about their rights and the legal steps they can take to protect themselves and hold the aggressor accountable.

Awareness and knowledge dissemination

- Providing educational resources and programs to raise community awareness about forms of digital violence and how to deal with them correctly and safely.
- Organizing workshops and awareness campaigns to combat digital violence against women by targeting groups of women, especially those in schools and universities.
- Building daily life skills.

Recommendations

To ascertain the provisions of the Constitution regarding equality, the preservation of personal freedom, and the safeguarding of individuals' privacy and to implement the commitments made by Lebanon in achieving sustainable development goals and the national plan to implement Security Council Resolution 1325 on Women, Peace, and Security, which was adopted by the government in September 2019, particularly in the context of combating gender-based violence. Some recommendations are presented below to protect the rights of women and ensure gender equality, which may include but are not limited to the following:

1. Joining international agreements:
   - Ratifying the Convention on Electronic Crime (Budapest Convention) in the realm of international collaboration, especially considering the transnational nature of cybercrime. The challenge of determining the jurisdiction of national courts emerges when the components of the offense are dispersed across multiple countries.
   - Joining the Council of Europe Convention aimed at Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention), which serves as the most comprehensive international legal framework for addressing and curbing violence against women and domestic violence.
2. Developing national legislation and strategies:

   The Lebanese legal system necessitates ongoing modifications to its cyber regulations to ensure compatibility with the swift advancements occurring within the information technology industry, with a particular focus on safeguarding personal data and combating electronic crimes, including those of significant importance such as the following:
   - Issuing a new special law that addresses instances of digital violence affecting both men and women, including digital blackmail, threats, bullying, and defamation, is a crucial aspect of contemporary legislation.
   - Amending the articles of the Lebanese Penal Code to incorporate a definition of digital violence and impose substantial penalties on individuals who commit digital violence offenses.
   - Amending the provisions of the Electronic Transactions and Personal Data Law No. 81/2018 requires a thorough review and amendment to ensure that it remains relevant in light of the technological advancements that have occurred over the past 18 years. The law, which was initiated in 2004, has not been updated to adequately address the issues of privacy and personal data protection that have arisen during this time. Furthermore, it is crucial to incorporate provisions that address various types of emerging cybercrimes that have emerged as a result of rapid development in this field.
   - Amending the provisions of the Code of Criminal Procedure No. 328/2001, which pertains to inspection procedures, evidence seizure, and confiscation, is necessary to ensure that the legal text is compatible with the new digital complexities. With the rise of digital crime scenes, it has become increasingly difficult to determine the identity of the criminal and the geographical location of the device used to commit the crime or to store digital evidence. The rapid pace at which evidence can be hidden or damaged, as well as the use of devices, internet protocols, identities, and digital addresses, have all contributed to this challenge. Therefore, it is necessary to update the legal framework to address these new digital complexities.
   - Amending Law No. 205/202 related to the criminalization of sexual harassment, particularly with respect to the protection of victims and witnesses, by introducing provisions that outline mandatory protection measures, methods, and mechanisms to be implemented.
   - Amending the articles of the Domestic Violence Law No. 204/2020 to encompass all instances of domestic violence, including marital rape, and to specify the methods or means by which the offense of domestic violence arises, as well as to designate a protective order for women and encompassing children under the age of 18 within the order and to strengthen penalties for perpetrators of the crime.
   - Conducting an analytical statistical study of the cases of digital violence referred to the Office for Combating Information Crimes and those presented before the relevant judicial authorities. This

endeavor aims to identify the basis for enacting a specific law or amending existing legislation to address digital violence. Furthermore, this study can assist policymakers in implementing appropriate measures to safeguard victims of digital violence.

- Conducting a comprehensive examination of the digital violence phenomenon, encompassing its various forms and the adverse outcomes it engenders for individuals and societies at multiple levels, with a particular focus on instances of digital violence perpetrated against women. This analysis serves as the foundation for constructing a comprehensive national strategy aimed at safeguarding cyberspace and ensuring its security.
- Undertaking the development of a national cybersecurity strategy for government institutions to follow in addressing cybersecurity challenges.[53]

3. **Enhancing the Capabilities of Frontliners:**
   - Enhancing the abilities of judicial institutions, particularly those associated with the criminal justice system, to address cybercrimes and utilize technological advancements.
   - Improving the proficiency of security agencies in delivering gender-sensitive training and offering victim-centered care while ensuring a safe space for reporting and pursuing grievances.
   - Qualifying the personnel of public institutions, specifically the Ministry of Education and the Ministry of Social Affairs, in handling cases of digital violence via hotline services and providing appropriate psychological, social, and legal support to effectively address these cases and collaborate with the relevant security and judicial authorities.
4. **Strengthening reporting and investigation:**
   - Women should be urged to disclose instances of digital violence to which they have been subjected or have witnessed and equipped with the necessary resources and facilities to do so, such as secure reporting and investigation mechanisms, and guaranteeing the confidentiality of investigations.
5. **Enhancing technology to track perpetrators of violence:**
   - Developing a digital forensics laboratory specialized in processing and analyzing digital evidence to activate the handling of digital evidence.
   - Establishing a national computer incident response center to address cybersecurity risks.
   - Developing techniques and mechanisms for prosecuting cybercrimes at the Anti-Cybercrime Office.
   - The procurement of contemporary and sophisticated information systems that aid security personnel, specifically the Anti-Cybercrime Office, in tracking down criminals and streamlining internal administrative operations to facilitate the monitoring of such crimes. For instance, the use of PILP,[54] which compiles digital identity information from various independent sources such as social media and email, to create a comprehensive picture of an individual's online identity and link it to their offline identity records. By collecting, linking, and verifying all aspects of identity data online, more precise digital identity information can be obtained, enabling the accurate monitoring of the criminal's identity and prosecution.
6. **Providing assistance services to victims of digital violence:**
   - Enhancing the provision of legal, psychological, and social support for victims by offering counseling services and establishing dedicated reception centers to assist victims in overcoming digital violence and addressing their difficulties.
7. **Cooperation between national institutions and international coordination:**
   - Establishing a collaborative effort and bolster cooperation between judicial and security agencies, public institutions, and civil society organizations to address violence against women and girls and achieve gender equality. This can be achieved by implementing programs and strengthening partnerships with nongovernmental organizations, ICT associations, and private institutions such as internet service providers and data service providers.

[53] No strategic vision for cybersecurity has yet to be developed in Lebanon, as no governmental institution has yet been created or appointed to deal with cybersecurity issues, http://www.tra.gov.lb/Cybersecurity-in-Lebanon-AR

[54] To learn more about the Pilp program, please visit the website https://pipl.com/

- Enhancing regional and international collaboration is crucial given that information crimes involve multiple components and often extend across national boundaries. Consequently, it is essential to establish a cooperative mechanism among countries to bolster concerted efforts in addressing digital violence against women.

8. Awareness and education:

Unceasing efforts should be made to educate society, particularly women, about the various forms of digital violence and how to address and report them:

- Disseminating information about the operations of security and public institutions, as well as their outcomes in combating diverse forms of violence against women and girls, particularly digital violence, is crucial for empowering women to resist attempts to undermine their dignity and for deterring potential perpetrators while also encouraging the reporting of violence incidents.
- Undertaking extensive awareness campaigns that target both girls and young men, specifically focusing on educational institutions such as schools and universities, as well as civil society, with the aim of:
  - Informing them of available methods for preventing cyber threats and protecting themselves.
  - Informing them of the reporting mechanisms available from various security and public institutions, as well as civil society organizations.
  - Informing them of the services and support that are available for victims of digital violence, which may include legal, psychological, and social assistance.
- The necessity of informing parents about the potential risks associated with the internet and instructing them on how to handle digital violence responsibly to ensure adequate protection for victims and to encourage the reporting and prosecution of perpetrators.
- Proposing the integration of educational resources for equality and counteracting gender-based violence within academic curricula.
- Improving the position of women in society and providing them with economic, social, and political empowerment to enable them to defend their rights and shield themselves from digital violence and other forms of violence.

Appendices

Appendix 1: List of Lebanese Legal Texts Related to Digital Violence Against Women

1. The 1926 Lebanese Constitution, including all its amendments.
2. Law No. 81 of October 10, 2018, which pertains to Electronic Transactions and Personal Data Protection.
3. The Lebanese Penal Code, established by Legislative Decree No. 340 dated January 3, 1943.
4. Law No. 164, enacted on August 24, 2011, which addresses Trafficking in Persons.
5. Law No. 293, enacted on May 7, 2014, which aims to protect women and other family members from domestic violence.
6. Law No. 205, enacted on December 30, 2020, which criminalizes sexual harassment and provides support for its victims.
7. Law No. 140, enacted on October 27, 1999, aims to preserve the confidentiality of intelligence gathered through any means of communication. This law was subsequently amended by Law No. 158, enacted on December 27, 1999.

Appendix 2: List of International and Regional Agreements

The following are among the foremost international and regional agreements designed to safeguard women, uphold their rights, and shield them from violence in general:

- The Universal Declaration of Human Rights and the United Nations Charter, both of which were adopted in 1948 and 1945, respectively, served as the foundation for the United Nations Convention on the Political Rights of Women, which was adopted in 1954. This convention emphasizes the principle of complete equality between men and women in the exercise and enjoyment of political rights, including the right to participate in the management of public affairs of one's country, either directly or through representatives, and to hold public positions. This principle is in line with the provisions of the United Nations Charter and the Universal Declaration of Human Rights.
- The United Nations Convention on the Elimination of All Forms of Racial Discrimination (CERD), which was adopted in 1963, seeks to eliminate racial discrimination in all its forms and manifestations, including cases of violence against women stemming from racial discrimination.
- The Declaration on the Elimination of Discrimination against Women of 1967, adopted in accordance with United Nations General Assembly Resolution No. (2263D-22),55 had the objective of taking all necessary steps to eliminate discriminatory laws, customs, regulations, and practices that affected women and to establish adequate legal protections for the equality of men and women in rights.
- The Declaration on the Protection of Women and Children in Situations of Emergency and Armed Conflict, adopted in 1974 under United Nations General Assembly Resolution No. 3318 (XXIX),56 affords special safeguards to women and children within the civilian populace in emergency and armed conflict scenarios. This declaration regards all forms of oppression and cruel or inhuman treatment directed at women and children as criminal acts.
- The Convention on the Elimination of All Forms of Discrimination Against Women, commonly referred to as the CEDAW Convention, was adopted in 1979 and is considered the most significant agreement in its field. The primary objective of this convention is to address and eliminate all forms of discrimination against women in various aspects of life, including political, economic, social, cultural, and civil fields. Additionally, the convention focuses on addressing discrimination that may result in violence against women.
- The Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women mandates the formation of a special committee, known as "the Committee," with the responsibility of eliminating discrimination against women. This committee has the authority to receive and assess communications that are submitted to it.
- The 1993 Declaration on the Elimination of Violence against Women, issued in accordance with United Nations General Assembly Resolution No. 408/104,57 calls upon states to denounce all forms of violence against women and to refrain from invoking any custom, tradition, or religious considerations as a means of avoiding their obligation to eradicate such violence. It is imperative that all necessary measures be taken, without delay, to eliminate violence against women.
- The Beijing Declaration, formulated during the Fourth World Conference on Women in 1995, serves to advance women's rights and realize the objectives of equality, progress, and tranquility for all women. Specifically, it targets all forms of violence against women, such as domestic violence and sexual exploitation. This document represents the international community's pledge to achieve gender equality and offer more favorable prospects for women and girls. This guarantees the ongoing

[55] To view the Declaration on the Elimination of Violence against Women of 1967, please see the electronic link: http://hrlibrary.umn.edu/arab/b021.html

[56] To view the Declaration on the Protection of Women and Children in Situations of Emergency and Armed Conflict of 1974, please see the electronic link: https://www.ohchr.org/ar/instruments-mechanisms/instruments/declaration-protection-women-and-children-emergency-and-armed#

[57] To view the Declaration on the Elimination of Violence against Women of 1993, please see the electronic link: https://www.ohchr.org/ar/instruments-mechanisms/instruments/declaration-elimination-violence-against-women

dedication of the international community to tackling civil, political, social, economic, and cultural disparities.

- Strategies and practical measures that were developed to eradicate violence against women in the realm of crime prevention and criminal justice, as outlined in the 1997 document "Model Strategies and Practical Measures to Eliminate Violence Against Women," were established in accordance with United Nations General Assembly Resolution 52/86.58 These strategies and measures are intended to guarantee de jure and de facto equality between women and men, as well as fair access to justice. Furthermore, these strategies aim to achieve gender balance in decision-making areas that are relevant to ending violence against women.
- The United Nations Convention against Transnational Crime, which was adopted in 2000, aims to address organized and transnational crime, particularly that involving acts of violence against women.
- The Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Particularly Women and Children, which complements the United Nations Convention against Transnational Organized Crime, was approved by the United Nations General Assembly Resolution 2000 and entered into force in 2002. This Protocol aims to prevent acts prohibited by Article 5 of the Protocol, investigate and prosecute the perpetrators, and safeguard the victims of such trafficking. This Protocol addresses transnational crimes and involves organized criminal groups.
- The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography, which became effective in 2002, is designed to safeguard children from all forms of violence and exploitation, particularly the sale and exploitation of children into prostitution and child pornography.
- The 2014 Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, commonly referred to as the Istanbul Convention, is a critical mechanism for addressing gender-based violence, such as domestic violence, rape, and sexual harassment. The convention serves as a potent instrument to safeguard asylum seekers who are vulnerable to gender-based persecution, including female genital mutilation.

The following text is a formal rephrasing of the original text, which affirms the principles of nondiscrimination and human rights. These principles are enshrined in the United Nations Charter of 1945 and the Universal Declaration of Human Rights of 1948. The Universal Declaration of Human Rights declares that all individuals are born equal in dignity and rights and are entitled to enjoy their rights and freedoms without any form of discrimination, including sex-based discrimination. In addition, there are various agreements and protocols that safeguard the protection of civil, political, economic, social, and cultural human rights. These agreements and protocols also emphasize the principle of nondiscrimination based on gender, race, color, language, religion, or social affiliation.

[58] To view model strategies and practical measures to eliminate violence against women, please see the electronic link: http://hrlibrary.umn.edu/arabic/ModelStrategiesViolenceWomen.html

Appendix 3: References and Sources

National Strategy for Women in Lebanon 2022-2030, National Authority for Lebanese Women. https://nclw.gov.lb/wp-content/uploads/2023/11/National-strategy-for-women-in-Lebanon-2022-2030-ar.pdf

A report on the implementation process of the "National Strategy Action Plan to Combat Violence against Women and Girls 2019-2029" is provided below. https://nclw.gov.lb/wp-content/uploads/2022/06/NCLW-VAWG-Stocktaking-Strategy.pdf

Gender Equality and the Legal System – Lebanon, February 12, 2023, UNFPA. https://arabstates.unfpa.org/ar/publications/gender-justice-and-law-lebanon

Electronic harassment: Tips for self-protection. United Nations UNITAD https://www.unitad.un.org/ar/bullyingcyber

Survey on digital violence against women in Lebanon, April 2023. Dr. Lubna Muhammad

"Crimes of defamation and defamation via the internet committed by a lawyer in 2022. (Oweidat, 2022)".

Lebanon's legislation on sexual harassment falls short in providing essential safeguards, according to a report published by Human Rights Watch in March 2021. https://www.hrw.org/ar/news/2021

Digital Evidence in the Judicial System: Lebanon Serves as a Model, according to a 2020 Study by Samer Abu Shakra.

Ensuring the confidentiality of personal information is a critical issue in today's world. A thorough examination of the current state of data protection and the obstacles that arise in the modern era is necessary. Dr. Hania Muhammad Ali Fakih, a renowned expert in the field, conducted an in-depth analysis on January 22, 2018, to understand the challenges faced in safeguarding personal information. http://77.42.251.205/LawRelatedResearches.aspx?lawId=257669

Ensuring Security in the Digital Realm and Counteracting Cybercrime: Proposed Policies, 2015, Economic and Social Commission for Western Asia (ESCWA). https://www.unescwa.org/sites/default/files/pubs/pdf/policy-recommendations-cybersafety-arab-region-arabic.pdf

Internet law pertains to the legality of social media behavior. In the fifth part of his analysis, lawyer Charbel Al-Qarih, a Doctor of Laws and former Chairman of the Informatics Committee at the Beirut Bar Association, explored this issue in 2013.

Internet law. Digital content for social networks. Part Six. Published in 2013 by Charbel Al-Qarih, a Doctor of Laws and former Chairman of the Informatics Committee at the Beirut Bar Association.

The challenge of identifying the cybercriminal and their location on social media networks was addressed by lawyer Charbel Al-Qarih in 2011. Dr. Al-Qarih holds a Doctor of Laws degree, and he formerly served as the Chairman of the Informatics Committee at the Beirut Bar Association.

Information crimes in the context of Lebanese law and jurisprudence, as examined by Judge Fawzi Khamis, President of the Legal Informatics Development Association in Lebanon.

The Economic and Social Commission for Western Asia (ESCWA) released guidelines in 2009 for coordinating cyber legislation in Arab countries. These guidelines covered two areas: the processing and protection of personal data and electronic crimes. They were created to provide guidance on how to address these issues in a coordinated and effective manner.
https://archive.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf

Lebanon Gender Equality Barometer: Cyber Extortion and Cyber Harassment. National Council for Lebanese Women (NCLW), 2023. https://nclw.gov.lb/wp-content/uploads/2023/03/LGEB_Cyber-Extortion-and-Cyber-Harassment.pdf

The mapping of legal frameworks and services for combating online and ICT-facilitated violence against women and girls in Arab countries was conducted by UNWomen in the year 2022.
https://arabstates.unwomen.org/en/digital-library/publications/2022/03/mapping-of-laws-and-services-for-online-and-ict-facilitated-violence-against-women-and-girls

The EDVAW Platform's seven mechanisms concerning the digital dimension of violence against women were examined in a thematic paper adopted by the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women at its 14th meeting on November 17, 2022.
https://www.coe.int/en/web/istanbul-convention/edvaw-platform

Violence Against Women in the Online Space. 2021. UNWomen.
https://arabstates.unwomen.org/sites/default/files/Field%20Office%20Arab%20States/Attachments/Publications/2021/11/Summary_Keyfindings_Final_EN.pdf