



THE LEBANESE DIGITAL VIOLENCE PREVENTION BILL POLICY RECOMMENDATIONS

Prepared by: Dr. Rouba El Helou¹
Supervised by: Hayat Mirshad



INTRODUCTION²

Lebanon lacks a comprehensive legal framework and protective mechanisms to address various forms of online violence, commonly referred to as "digital violence." Studies show that women and girls are the most vulnerable to such abuse, which includes sexual threats, the non-consensual sharing of intimate images, and cyber harassment³. Without effective measures to combat digital violence, victims remain unprotected, while perpetrators often evade accountability, exacerbating the harm to individuals and society⁴. Despite efforts by Lebanese lawmakers to introduce legislation on defamation, libel, and workplace harassment, significant gaps remain. The passing of Law No. 205 in December 2020, which criminalized sexual harassment and provided for victim rehabilitation⁵, was a step toward modernizing Lebanon's legal landscape. However, digital violence continues to rise, affecting women, children, and seniors alike⁶.

Compounding the issue is the absence of a clear and consistent global system for reporting online violence. Additionally, the inherently decentralized and borderless nature of the digital world makes regulation and enforcement even more challenging. Human Rights Watch has recognized Law No. 205 as a positive step, highlighting its provisions that protect victims "from retaliation, including in pay, promotion, transfer, contract renewal, or disciplinary measures". However,⁸ while it represents progress in criminalizing such behavior, Human Rights Watch noted that the legislation falls short by not directly linking it to labor law reform, oversight mechanisms, civil remedies, preventive measures, and workplace protection policies. The law also includes safeguards for individuals who report harassment and prohibits discrimination against them.⁹



¹ Rouba El Helou, university lecturer, gender, human rights & communication expert She is currently the FORGE-Fellow in the Future of Rights and Governance program at New York University (NYU) School of Law, researching and working on a project titled "Human Rights of Human Resources (HRofHR)". She also serves as the Secretary General and a member of the Executive Board of the Lebanese Center for Human Rights (CLDH). She has an extensive experience in media and organizational development, with a particular focus on fact-checking, strategic planning, policy design and implementation, and structural reforms. As both an academic and a practitioner, she has developed numerous training tools and publications on Open Educational Resources (OER), in addition to works on organizational reform, communication in the network society, and peer-reviewed articles in feminist and masculinist studies, postcolonial and intersectional cultural studies, and autoethnography. Her research interests include political communication, gender-based violence, intersectional gender studies, media self-organization, digital rights, and rule of law governance. Rouba is also active as a journalist, lecturer in communication and gender, and consultant in academic planning and quality assurance in higher education and training. She has worked extensively across the media sector on communication strategy, organizational development, policy reform, and media systems.

² Note: This policy paper was reviewed by experts in digital surveillance, digital rights, feminism, and human rights to ensure that the research focus and recommendations are based on a participatory approach, inclusivity, and practical. The researcher expresses her gratitude to: Samar Al Halal, digital rights and security expert; Nourhan Abu Zeid, lawyer and feminist activist; Abed Kataya, digital content manager at SMEX; Nourhan Sharafeddine, communications and advocacy staff at the Lebanese Center for Human Rights; Dalal Saoud, journalist and regional adviser for Women In News; and Mayada Abdullah, project coordinator of the Arab Master's Program in Democracy and Human Rights at Saint Joseph University and member of the LADE board, for their invaluable review and support throughout the research process.

³ Program in Democracy and Human Rights at Saint Joseph University and member of the LADE board, for their invaluable review and support throughout the research process.

⁴ <https://onlineviolencewomen.eiu.com/>

⁵ <https://www.amnesty.org/en/what-we-do/technology/online-violence/>

⁶ <https://blogs.worldbank.org/ar/arabvoices/sexual-harassment-workplace-lebanon-where-are-we-headed>

⁷ Song, Haoming and Holzer, Angie (2023) "Online Safety Laws by Country," Journal of Nonprofit Innovation: Vol. 3: Iss. 3, Article 3. URL: <https://scholarsarchive.byu.edu/joni/vol3/iss3/3>



On a global level,¹⁰ the Online Safety Act 2023 in the United Kingdom (UK) serves as an important legislative model for Lebanon. This law aims to protect both children and adults in the digital space while holding social media companies and search services accountable for user safety on their platforms. It introduces a new set of obligations, including protecting users of all age groups, preventing harmful content, and providing reporting mechanisms. It also mandates major platforms to be transparent about the types of content they allow, and it gives users greater control over the content they view.

The UK's communications regulator, Ofcom, is responsible for enforcing the law as an independent oversight body. It monitors compliance, publishes codes of conduct and guidelines for companies subject to the law, and has broad authority to assess platforms' adherence to regulations. Ofcom can also impose penalties and substantial fines, including on service providers outside the UK if they operate within or have links to the country.

The implementation of laws similar to the Online Safety Act in Lebanon faces significant challenges. These include the need for advanced technological infrastructure, such as specialized applications and software, as well as the risk of these tools being misused against activists.

Additionally, legal complexities in defining hate speech, concerns over government surveillance, and the challenge of balancing accountability with individual privacy protections further complicate the process.

In this context, online "targeted advertisements" (Targeted Ads) have emerged as a powerful tool for political disinformation, raising concerns about the influence of digital platforms on elections and their outcomes.

This research aims to propose policies and visions that support legal and protective measures for Lebanese society, while drawing on international experiences, such as those of the UK, and considering the challenges of implementation in the Lebanese context.

Ultimately, we cannot embark on a path to effectively combat digital violence in Lebanon without adopting a comprehensive, participatory, and multi-stakeholder approach, which requires institutional, technical, and financial prerequisites.

This can be achieved through organizing focused parliamentary debates with public accessibility for everyone.

Strengthening trust, and enhancing cooperation between public and private institutions, alongside securing the necessary budget for law enforcement. Beyond that, regarding transparency and accountability, there is a need for an open public dialogue with civil society communities. Furthermore, there is a need to set an agenda, make and implement decisions, and ensure the transparency of their application to all stakeholders."

⁷<https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/114675/205.pdf>

⁸<https://www.hrw.org/ar/news/2021/03/05/378078>

⁹<https://www.openglobalrights.org/human-rights-of-human-resources-workplace-justice-in-lebanon/>

¹⁰<https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#what-does-the-online-safety-act-do>



WHAT IS OUR GOAL?

This research analysis aims to establish a framework for a public policy that contributes to protecting internet users in Lebanon from digital violence. This will be achieved by establishing clear preventative mechanisms, outlining an effective regulatory approach to address these crimes, and identifying key stakeholders and involving them in finding sustainable solutions.

Digital violence can discourage participation in public online discussions, particularly among women, leading many to avoid using social media or freely expressing their opinions. This, can also negatively affect their opportunities, for education, employment, and political participation

Lebanon's weak record in policy reform and implementation poses a significant challenge. However, we can leverage the modest experience in the media sector's self-regulation as a model for comprehensive reform. A successful reform initiative can be a starting point for change in other areas. As the saying goes, 'a journey of a thousand miles begins with a single step'; and to achieve this and witness change, we must overcome the obstacles of toxic sectarianism, impunity, and the deeply rooted patronage system in Lebanon. This paper provides a set of guidelines to initiate a national dialogue on very specific and vital areas for action in the digital policy reforms.

Digital violence

can discourage participation in public online discussions, particularly among women, leading many to avoid using social media or freely expressing their opinions. This, can also negatively affect their opportunities, for education, employment, and political participation

Lebanon's weak record in policy reform and implementation poses a significant challenge.

However, we can leverage the modest experience in the media sector's self-regulation as a model for comprehensive reform. A successful reform initiative can be a starting point for change in other areas. As the saying goes, 'a journey of a thousand miles begins with a single step'; and to achieve this and witness change, we must overcome the obstacles of toxic sectarianism, impunity, and the deeply rooted patronage system in Lebanon. This paper provides a set of guidelines to initiate a national dialogue on very specific, vital areas for action in the digital reform field."

Lebanon's weak track record in policy reform

and implementation poses a major challenge for us. However, the country's modest experience in media self-regulation¹¹ can serve as a foundation for broader comprehensive reform. A well-executed digital safety initiative could pave the way for change in other areas.

As the saying goes, 'a journey of a thousand miles begins with a single step'; and to achieve this and witness change, we must overcome the obstacles of toxic sectarianism, impunity, and the deeply rooted patronage system in Lebanon.

This paper provides a set of guidelines to initiate a national dialogue on very specific, vital areas for action in the digital reform field."

Digital Violence and International Challenges

While technology is a powerful tool for empowering internet users and advancing rights, it is increasingly being used as a means to perpetrate violence against women, through harassment, discrimination, and cyberbullying. This digital violence is an extension of structural discrimination against women, amplified by the characteristics of the internet, creating new challenges in the field of digital rights¹². To effectively address these issues, we need comprehensive policies that narrow the digital gender divide by ensuring equal access to technology, enacting laws that prosecute cyberviolence, raising awareness about the dangers of digital violence and its social impact, enabling all gender identities to use technology safely and freely, while ensuring that cybercrime laws are not used as a tool of suppression and silencing voices¹³.

While the global nature of the internet poses significant law enforcement challenges, and perpetrators may reside in different countries, making it difficult to apply national laws effectively. Laws specific to online harassment are essential to overcoming these legal complexities and ensuring cross-border cooperation to hold harassers accountable.

The Concept of Digital Violence: Its Inclusiveness and Limitations

While the term 'digital violence' encompasses various types of gender-based violence (GBV) facilitated by technological tools and digital devices, such as mobile phones, internet Apps, email, or through social media platforms; it often overlooks the gender-intersectional dimension and diverse identities, as well as the social and cultural classes of digital societies¹⁴.

¹¹For three years, the researcher worked on the implementation of media self-regulation in Lebanon with several local organizations and sectors. This experience can serve as an example for the future.





Digital Violence in Arab States: Reality and Challenges

The 2022 UN Women – Arab States report, Mapping of Laws and Services for Online and ICT-Facilitated Violence against Women and Girls in Arab States, examines existing legislation and support services addressing online violence against women and girls in the region. It also highlights international frameworks and best practices for combating ICT-facilitated violence.

The report finds that while no Arab country has enacted specific laws addressing online violence, governments have generally adopted a three-pronged legal approach to regulating digital spaces:

1. Expanding domestic violence laws to include online violence.
2. Enacting comprehensive legislation against all forms of violence against women (e.g., Tunisia's 2017 law).
3. Implementing cybercrime laws to address digital offenses.

Despite these positive advancements, The UN Women- Arab States report on mapping of laws indicates that online violence is often viewed solely as a cybercrime, which can lead not only to neglecting the specific needs and rights of women, girls, but also all gendered intersectional identities. Furthermore, cybercrime laws may lead to violating privacy and restrict freedom of expression.

To date, 13 Arab countries have enacted cybercrime laws that include provisions on online violence against women and girls. These include Algeria, Bahrain, Egypt, Jordan, Kuwait, Libya, Oman, Qatar, Saudi Arabia, the State of Palestine, Sudan, Syria, and the United Arab Emirates. The remaining nine Arab states have either lack implemented general cybercrime laws or have yet to take significant legal action on the issue¹⁵

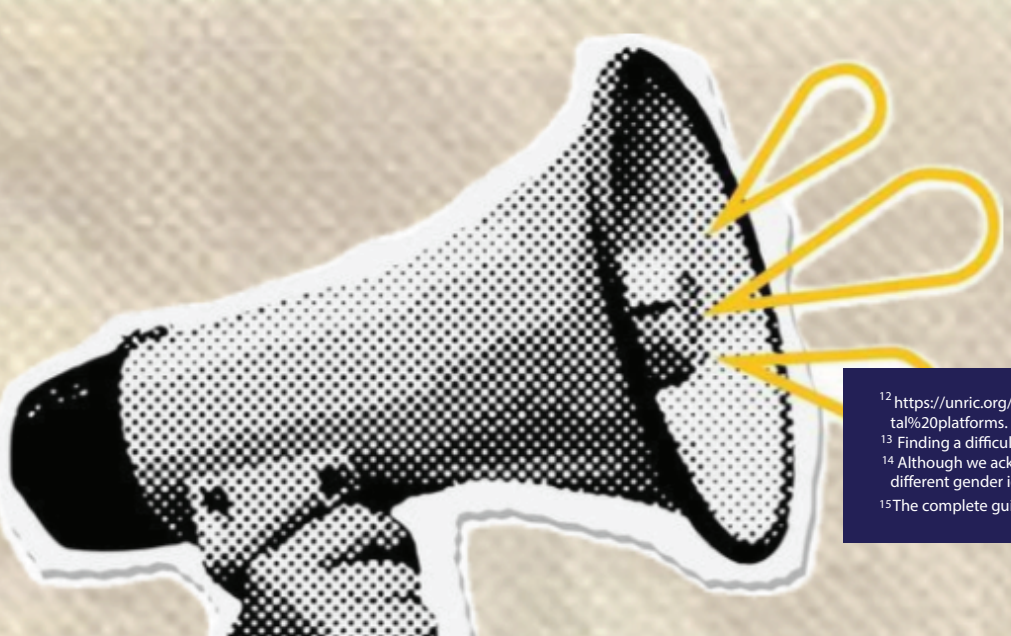
Digital Violence: A Growing Phenomenon in Lebanon

The global rise in digital violence is an alarming phenomenon, and Lebanon is no exception. This escalating issue threatens individual safety and fundamental rights, particularly freedom of expression and privacy. However, addressing this challenge does not mean restricting digital technologies. On the contrary, technology remains a powerful tool for positive change, but its misuse, whether through abuse of power, discrimination, bullying, or marginalization, can cause significant harm.

A lack of digital literacy can turn these tools into instruments of control and oppression.

Therefore, as part of our social and national responsibility, we must bridge the gap between technological advancement and legal frameworks while ensuring clear protections for victims.

Understanding the history, potential, and risks of information and communication technology (ICT) is essential to aligning its rapid evolution with effective legal safeguards.



¹² <https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/#:~:text=Studies%20across%20the%20world%20show,and%20reach%20of%20digital%20platforms.>

¹³ Finding a difficult balance: Human rights, law enforcement and cyber violence against women | GenderIT.org

¹⁴ Although we acknowledge that women are the most vulnerable to gender-based violence, it is important to remember that gender-based violence does not exclude anyone. It affects different gender identities (including non-binary and non-symmetrical), including children and men in certain contexts.

¹⁵ The complete guide: <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>

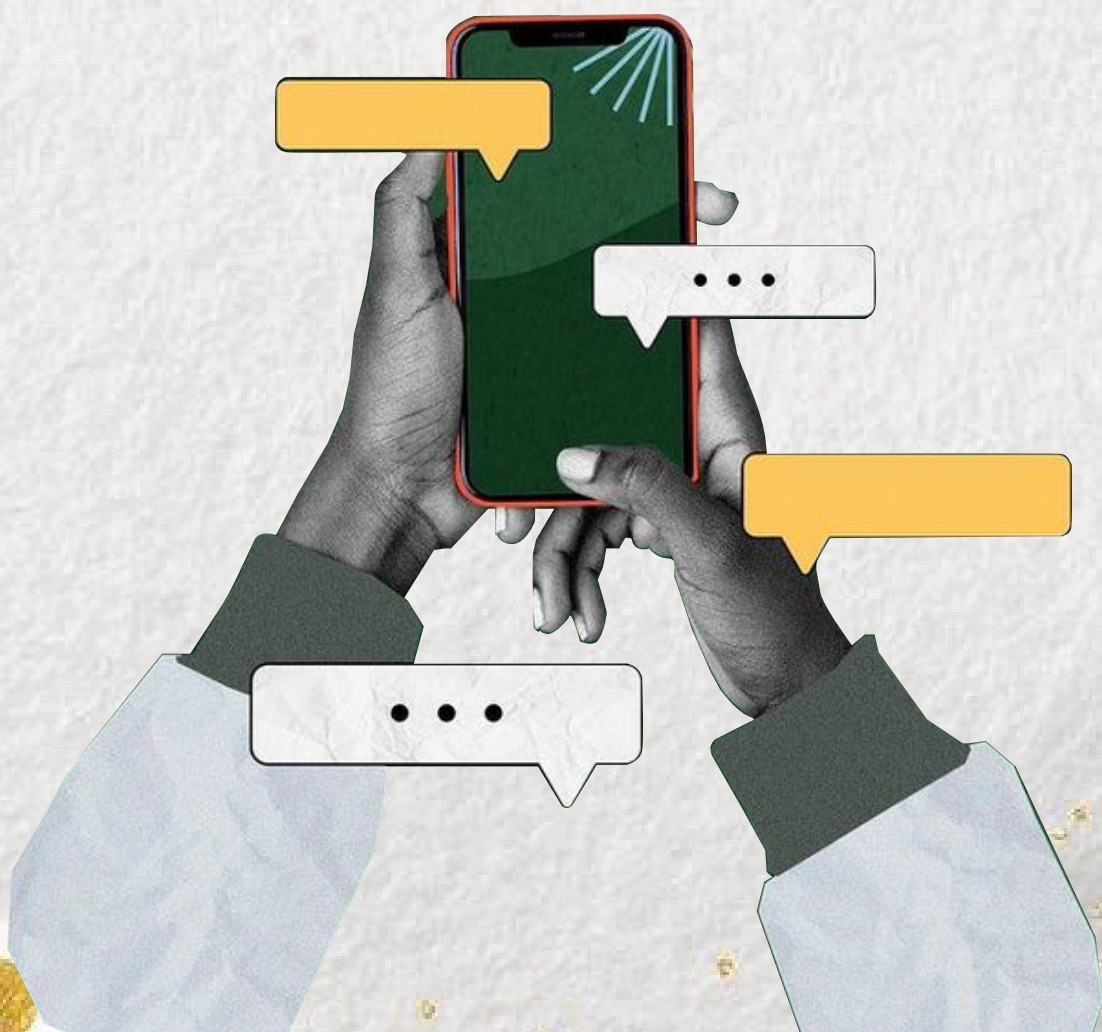
This does not mean that we should prevent the use of digital technologies and their tools, because we cannot and should not neglect the role and importance of technology as a driver of positive change around the world. However, a lack of awareness in the areas of its use can make it a tool for control and harming others through the misuse of power, discrimination, bias, as well as bullying and marginalization. We believe, as part of our social responsibility, that understanding technological capabilities and aligning them with legal frameworks, and providing clear and accessible protection for victims, is an important and essential part of our national duty first, and our humanitarian duty second. We are concerned with understanding information communication technology—its history and capabilities—as well as aligning its rapid progress with laws.

Digital Violence as a Tool for Control;

The Need for a Law to Combat it Protection

We also highlight violence as censorship and control tool against many individuals, especially women, in Lebanon and in the digital space. This includes physical, sexual, and psychological violence, as well as online violence such as harassment, cyber-bullying, which forces many women to impose self-censorship or withdrawal from public platforms. This negatively impacts their participation in public discussions, limits their freedom of expression, and undermines their opportunities for education, employment, and political participation.

Studies indicate a worrying rise in online "sextortion" complaints in Lebanon (increased by 307% in 2020¹⁶), emphasizing the urgent need for a public policy framework that contributes to **protecting internet users, especially women and girls, from digital violence**. This includes providing clear preventive mechanisms and outlining an effective regulatory path to address these crimes, identify stakeholders and ensures their engagement in finding sustainable solutions. This research emphasizes **the importance of addressing gender-based control in all its forms, which constitutes a violation of human rights and a threat to the full effective participation of women in society**.



¹⁶<https://globalvoices.org/2021/03/10/online-rape-threats-connect-lebanese-activist-to-thousands-of-other-women-facing-abuse/>



Policies, Media Literacy, and Freedom in the Digital Space: Are There Any Practical Recommendations?

From this perspective, we deemed it appropriate for this research paper to address how to link and align **corporate policies with local laws; and how to disseminate a culture of media and information literacy to female and male citizens in general, as well as to female and male internet users**, and every person residing in Lebanon.

It also highlights a set of increasing digital threats, such as viruses, data theft, and electronic fraud, especially with the development of artificial intelligence applications and the Internet of Things (IoT), and the potential technical vulnerabilities that may arise within them. These vulnerabilities make it easier for hackers to exploit personal data or use it for unethical purposes, which threatens individuals' privacy and exposes them to the risk of blackmail or digital violence. The paper provides an analysis of the **various types of digital crimes** committed online and through social media, recognizing that it is difficult to list them all due to the constant evolution of the digital world. The paper also highlights a set of increasing digital threats, such as viruses, data theft, and cyber fraud, especially with the development of artificial intelligence (AI) applications and the IoT, and the potential technical vulnerabilities that may arise within them. These vulnerabilities make it easier for hackers to exploit personal data or use it for unethical purposes, which threatens individuals' privacy and exposes them to the risk of blackmail or digital violence.

In this context, the paper offers a set of recommendations aimed at creating a safe and fair public space for all, by emphasizing the principles of net neutrality, personal data protection, digital security, and the economic dimension.

Just as we have sought freedoms in all their forms and the necessity of providing a safe and fair digital environment for all. We identify many types of crimes that occur online and on social media, while acknowledging the difficulty of enumerating them all due to the continuous development of the digital world. We also see that digital violence, which includes violations of privacy and threats to personal security, both physical and psychological, and may extend to economic violence, all of which requires a legal framework to protect individuals and society in all their gender identities, social classes, ages, and persons with disabilities, as an intersectional approach to these identities. We present recommendations for what we dream of as a public space for all, far from abuse of power, fraud, and violence, as well as digital threats such as viruses, data theft, and electronic fraud, with the development of applications and those related to AI, IoT, and the vulnerabilities that may appear in them. These vulnerabilities make it easier for hackers to exploit personal data or use it for unethical purposes, which threatens individuals' privacy and exposes them to the risk of blackmail or digital violence. In this context, we present through this analysis a set of recommendations aimed at creating a safe and fair public space for all, by emphasizing the principle of 'Net neutrality'¹⁷, the protection of personal data¹⁸, digital security, while taking into account the economic dimension.

The Existing Situation and the Rational Behind the Proposed Legislation

Human Rights in the Digital Space: Challenges and Opportunities

Human rights are universal, interdependent, indivisible, and inalienable, enjoyed by all individuals regardless of where they live, their gender identity, or their religion, culture, or ethnic background¹⁷. These rights that people enjoy outside the cyberspace (offline) are the same rights that must be protected within the cyberspace as well.²⁰ Just as every individual has the right to enjoy a safe digital space, the rapid development of the internet poses challenges related to cybersecurity.

Just as every individual has the right to enjoy a safe digital space, the rapid advancement of internet poses cybersecurity challenges. Cyberattacks, the exploitation of personal data, and digital violence underscore the need to develop a digital policy approach that takes into account personal and collective rights and freedoms. The digital environment offers immense opportunities for the promotion human rights, learning and development, but it also poses new risks if not properly monitored and regulated. For instance, policies aimed at enhancing children's online safety are necessary should consider measures to ensure age limits and avoid potential impacts on other human rights such as invasion of privacy and other harmful behaviors that may pose an ongoing threat to privacy and rights.

The digital environment offers tremendous opportunities to promote human rights, learning, and development, but it also poses new risks if these are not heeded and this space is not appropriately regulated. For example, policies aimed at promoting child safety online must consider measures to ensure age verification and avoid potential impacts on other human rights, such as the violation of individual privacy and other harmful behaviors that may pose a continuous threat to privacy and rights.



¹⁷ Net neutrality ensures that all internet data is treated equally by Internet Service Providers (ISPs) and governments, regardless of the content, user, platform, application, or device. However, we need to look beyond the question of whether internet platforms should be regulated to examine how they should be regulated and what models truly ensure safety for users, not just superficially. This concept is crucial when drafting legislation, especially to activate trust, justice, transparency, and the non-blocking of the network, no matter the necessity.
¹⁸ By Personal data we mean data that relates to a person's private life, such as political leanings, religious beliefs, or financial transactions, etc. The protection of this data is of utmost importance in light of the development of modern and the creation of information storage units (or data warehouses).
¹⁹ <https://www.ohchr.org/ar/what-are-human-rights>
²⁰ <https://www.ohchr.org/en/topic/digital-space-and-human-rights>

Balancing The Protection of Rights and Freedom of Expression

As states strive to protect rights associated with online safety by removing harmful content, this may conflict with freedom of expression. In Lebanon, policymakers must carefully assess the human rights implications of digital policies, ensuring that digital transformation is people-centered and rights-oriented rather than restrictive.

Therefore, policymakers in Lebanon must consider the impact of digital policies on human rights to ensure that people are at the center of digital transformation and that it is rights-oriented. Technology has a positive impact on communication, education, health, and commerce, as well as global mobility, but it also poses challenges such as privacy issues, over-reliance, and the digital divide. Therefore, it is necessary to leverage the potential of technology responsibly and work to address its challenges to ensure a better future for everyone in Lebanon.

Cultural legacies of stereotypical gender roles, discriminatory laws and policies, misogyny, and gender discrimination contribute to the marginalization of women's voices and suppression of their freedom of expression, especially in the digital space.

This situation is exacerbated in Lebanon, where statistics show that women and girls make up the vast majority of cyber violence victims²¹, affecting their full participation in public life. Therefore, it is urgent to create laws that combat this violence and establish a gender-based approach to protect all internet users, especially women, in light of the rise and challenges of cybercrime.

These violent activities include data theft, threatening messages, privacy issues and cyberbullying targeting women in politics and business, discouraging them from public participation²². We argue in this research paper that these violent behaviors and transgressions not only undermine the credibility of networks, but also reduce the reliance on technology as a key enabler of women's empowerment in entrepreneurship, remote work, and political participation. This reality leads to a massive exclusion that constitutes a major imbalance in society. Globally, digital crime patterns have diversified, with more than 30,000 cybercrime incidents detected worldwide between November 2022 and October 2023.



²¹ <https://www.statista.com/topics/9384/gendered-abuse-online/#topicOverview>

²² For more information read the following: <https://www.skeyesmedia.org/ar/News/News/08-03-2023/10537>

The 'FEMALE' organization has been documenting the number of cybercrimes committed against women and girls in Lebanon. The recorded cases reached 1,123 in 2018, 1,270 in 2019, and 315 in the first quarter of 2020; marking a 184% increase over time. These numbers continue to rise, as the percentage of complaints related to cybercrimes through the Internal Security Forces (ISF) online service called 'Balegh' (meaning report) show that in 2022, women submitted 70% of complaints and 67% in 2023²³. Despite the lack of comprehensive, gendered lens local studies and reports on cybercrime, we can infer that the reason for the high percentage of complaints filed by women in Lebanon is due to their increased awareness of their rights, the growing number of internet users, the availability of cybercrime reporting services by local organizations and awareness campaigns, in addition to their increased exposure to online violence.

2. Justifications:

Despite the importance of privacy protection in the digital age, **current Lebanese legislation lacks a clear definition or comprehensive protection mechanisms** for this concept through any contemporary definition, leaving the matter to judicial interpretation.

Article 14 of the Lebanese Constitution (May 23, 1926) stipulates that "The place of residence is inviolable. No one may enter it except in the circumstances and manners prescribed by law". As for the term "freedom," it is mentioned in Articles 8 and 13, where Article 8 indicates that "personal liberty is guaranteed and under the protection of the law"²⁴, while **Article 13 includes** freedom of expression, opinion, and assembly. The preamble of the Lebanese Constitution also pledges **Lebanon's affiliation with the United Nations (UN) and its adherence to its charters, the Universal Declaration of Human Rights**²⁵ (issued in 1948), and **the International Covenant on Civil and Political Rights (ICCPR)**²⁶. **The Universal Declaration of Human Rights enshrines this right to privacy in Article 12**, which prohibits arbitrary interference in individuals' private lives and guarantees legal protection against such interference.

At the level of the European Union (EU), and with regard to the General Data Protection Regulation (GDPR) for example, the regulation includes a comprehensive law for the protection of personal data (issued in 2016 and entered into force on May 25, 2018), provides individuals with greater control over their personal data and the ability to correct or delete it. It also provides the right to data portability and objection to its processing, and unifies data protection laws across all member states of the Union. The law also obliges organizations to be transparent and obtain consent for any use of information, with the appointment of a data protection officer, the reporting of breaches, and the application of significant financial penalties in the event of their occurrence. Returning to Lebanon, it is worth mentioning that when the Lebanese Constitution was drafted in 1926, it was not anticipated that the concept of freedom and personal life would extend beyond the rights known at that time to include what has become commonplace today in the age of information technology and digital development. Four key elements of privacy can be summarized as follows:

1

Physical privacy: Protecting individuals from physical abuse;

2

Communications privacy: The right of individuals to maintain the confidentiality of their communications, including emails and phone calls;

3

Spatial privacy: Protection of the sanctity of the home and the regulations governing searches in private and public places;

4

Information privacy: Regulating the management of personal data on electronic devices and the Internet, allowing individuals to control their personal information such as health, financial, and social data, and determine how others access this information, whether it is stored on email or social media platforms. This is a sensitive issue, given the potential for users to share their information without considering aspects of privacy and control.

²³ <https://tinyurl.com/ecys3w74>

²⁴ <http://77.42.251.205/LawArticles.aspx?LawTreeSectionID=263836&lawId=244058&language=ar>

²⁵ <https://tinyurl.com/Universal-Declaration>

²⁶ <https://www.ohchr.org/ar/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

The Lebanese Electronic Transactions and Personal Data Law (also known as Law 81/2018) was issued on October 10, 2018²⁸, as a unique law in Lebanese legislation aimed at addressing cyber-legal matters from civil, commercial, and penal terms.

In February 2024, the Samir Kassir Foundation (SKF), in collaboration with SEEDS for Legal Initiatives organization, published a report titled²⁹ "Towards a Modern Personal Data Protection Law in Lebanon". The report emphasizes the necessity of adopting fundamental amendments regarding the protection of privacy and personal data.

It also describes the current law as outdated, with ineffective provisions for data protection in the present time. Furthermore, it argues that the law is not comprehensive, does not fully consider the principle of "individual autonomy," and does not require the data subject's consent for the processing of their data. The report also mentions that compliance with the law is very limited and that it is violated by political forces and figures during various times, such as election campaigns. A detailed analysis of data protection frameworks is of paramount importance in the context of digital violence, particularly gender-based violence. Data protection contributes to safeguarding victims by preventing the sharing of their sensitive information that could be used to harm them, especially women and girls who are more vulnerable to online violence, as well as marginalized and vulnerable individuals. These frameworks also provide a pathway for holding perpetrators accountable, particularly in cases of gender-based violence such as harassment and stalking. Furthermore, these mechanisms contribute to building trust and encouraging victims and whistleblowers to report and seek support.

Combating Digital Violence: Gender Mainstreaming and Intersectionality

In this context, we see, and after reviewing reports and laws, that updating and revising the law, based on the concept of Gender Mainstreaming and Intersectionality policies, is a national responsibility. It contributes effectively to addressing online violence, particularly gender-based violence. **Understanding digital violence and its roots is essential to addressing its causes**, as is understanding technological and informational development and linking the two concepts is essential for lawmakers. Cyberviolence is rooted in cultural legacies that have long existed outside of the digital world, only to be transmitted into it and contribute to the reinforcement of discrimination and abuse of power as a surplus of power that allows the reality of domination to be extended online. One of the main causes of online violence may be the unregulated transfer of social norms that justify aggressive behavior from the real world to the digital space.

A lack of awareness of digital safety may exacerbate the spread of these behaviors, as victims may be reluctant to talk about harmful experiences or not know how to seek help. We also face a lack of legislation, a lack of keeping up with the rapid technological development, and a lack of expertise in this field. Working on media and information literacy (MIL) is an essential framework for developing policies and projects in this situation. By enhancing critical thinking skills, encouraging responsible digital citizenship, and creating inclusive spaces to create an intersectional digital environment with a protective, safer, and more respectful approach for all, MIL is integrated into national programs in the public and private sectors. Accordingly, it is necessary to create laws that protect against digital violence. It should be a legal framework that is intersectional, inclusive, and based on human rights and freedoms, including:

- **Anti-Cyberbullying Laws:** These encompass harassment and bullying across digital platforms, extending to all forms of digital violence. They should also protect whistleblowers of these crimes, provided the primary goal is the public interest. They also protect the victim from retaliation or revenge if they file a complaint.
- **Data Protection and Privacy Laws:** Including addressing privacy violations such as sharing photos or personal data without permission.
- **Hate Speech and Incitement Laws:** Anything that results in digital violence, such as content that incites violence or hatred against individuals based on their personal characteristics like race, gender, sexual orientation, or other characteristics. Given the rapid spread of such content, clear legal definitions and enforcement mechanisms are necessary. Such speech spreads rapidly in the digital environment.

²⁷ Hania Mohammad Ali Fakihi. Protecting the Right to Information Privacy: An Analytical Study of the Current Protection Landscape and Contemporary Challenges". Electronic link: <http://77.42.251.205/ViewResearchPage.aspx?id=57&language=ar>

²⁸ <http://legiliban.ul.edu.lb/Law.aspx?lawid=278573&language=ar>

²⁹ https://www.skeyesmedia.org/documents/bo_filemanager/Data-Protection-Report_AR.pdf



In Lebanon, no act can be considered a crime or penalized unless there is a clear legal text defining it. Therefore, penalties cannot be imposed for actions not clearly defined by law, hence the need for a legal text that specifies its elements and the resulting penalties. The current Lebanese Penal Code, which was established in the 1940s, does not include provisions related to cyber privacy violation crimes, which complicates the issue of punishing perpetrators of these crimes in light of technological development. Meanwhile, defamation in the digital space allows the dissemination of offensive or false information online with the aim of harming someone's reputation or defaming them.

This type of crime is characterized by its rapid spread and ease of access to a wide audience, which increases the severity of the harm that can be inflicted on an individual, necessitating the development of modern laws that keep pace with these modern challenges. Online libel and slander crimes are among the modern legal challenges in Lebanon, as the internet is considered a public means that enables the widespread dissemination of insults and defamation, potentially reaching millions of people through social media platforms and email. This raises questions about the possibility of applying the provisions of the Lebanese Penal Code, particularly Articles 582 and 584, related to libel and slander crimes, to actions committed online. This issue also raises the need to consider whether the internet is considered a means of publication according to Article 209 of the Penal Code, in addition to the necessity of regulating the judicial jurisdiction to consider lawsuits of libel and slander committed online.

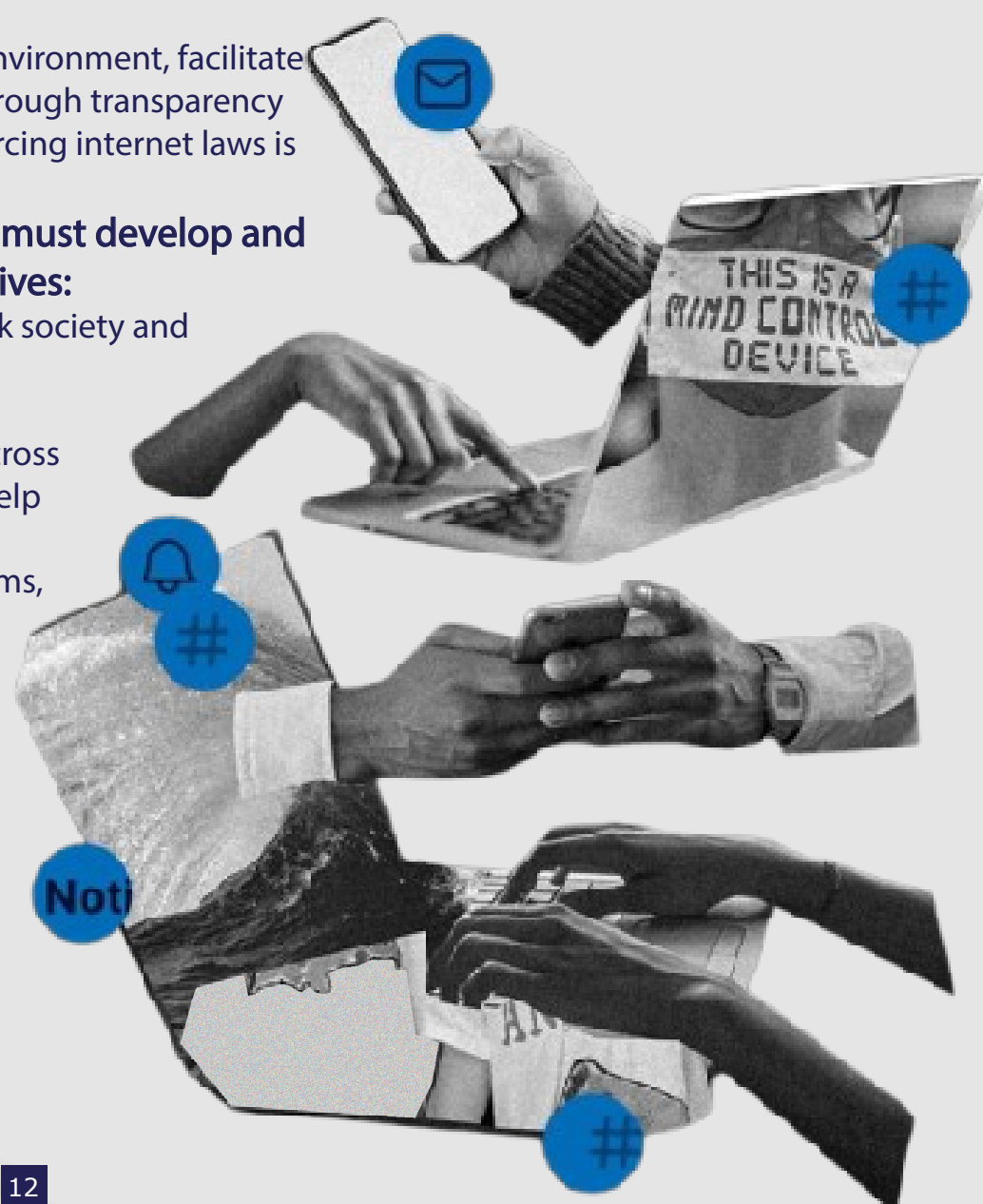
Towards a Safe Digital Environment in Lebanon: Lessons from the Digital Services Act

After much anticipation, the Digital Services Act (DSA), was issued October 2022 and entered into force on August 25, 2023, in all European Union countries (19 countries officially). The law is a set of regulatory foundations aimed at protecting users from harmful content such as violence and compelling major platforms to address these issues more effectively. The importance of this law lies in its establishment of a potential global standard for platform governance, through which the Lebanese legislator can work on a similar arbitration model. It also holds platforms fully responsible, upon its complete implementation, for the societal risks arising from the use of their services and the need to be more transparent about how their algorithmic systems work and protecting their digital community.

Despite the challenges, the law is expected to provide a safer environment, facilitate the reporting of violence, protect victims, and promote trust through transparency and accountability. Therefore, we see that developing and enforcing internet laws is vital for several reasons:

To ensure a secure and inclusive digital space, Lebanon must develop and enforce modern internet laws with the following objectives:

- Providing Legal Protection for of all identities in the network society and guaranteeing their rights to privacy and safety.
- Providing preventive and deterrent legal frameworks
- Activating self-regulatory mechanisms for accountability across multiple departments and national executive authorities that help hold perpetrators accountable and provide justice for victims.
- Offering legal protection and psychological support to victims, including legal resources, legal aid and protection measures.



What Are the Main Points Proposed in the Current Research and What Is the Proposed Legislative Framework?

A. Defining Digital Violence and What Constitutes Criminalized Acts

Definitions related to digital violence are numerous. Below is an overview of some of these definitions and the most important terms.

Digital violence is a global and growing phenomenon. It encompasses a range of harmful behaviors committed through digital means. While each country has its own context and different forms of this phenomenon, including electronic surveillance, hacking personal accounts, and the dissemination of private photos without consent, all aimed at controlling or harming the victim.

Unfortunately, there is a significant lack of comprehensive research on digital violence in Lebanon and in many other countries. This hinders the understanding of the experiences of victims and develop effective responses. However, by identifying the most common types of digital violence, we can work to provide knowledge and legal solutions.

These acts include privacy violations, online abuse, exploitation, incitement and hate speech crimes, and threats of physical violence.

Nevertheless, this type of violence leaves deep negative impacts on its victims, potentially leading to depression, weakened or lost self-confidence, anxiety, and social isolation. It also contributes to creating an unsafe and toxic digital environment, far from freedom. This reality requires multi-level responses to address it, from prevention and awareness to legal intervention to protect victims, establish a deterrent path, and build a safer digital society for all.

Herein lies the importance of the definition provided by the United Nations Population Fund (UNFPA) in its 2021 Tip Sheet on Reporting Digital Violence: A Practical Reference Guide for Journalists and Media: "any act of violence perpetrated by one or more individuals that is based on gender inequality and gender norms and is committed, assisted, aggravated and amplified in whole or in part using ICTs or digital media, against a person on the basis of their gender."

It is perhaps necessary to understand power relations and analyze their dynamics from a gender perspective for a more effective in-depth understanding of digital violence, that is, by transforming every action and every campaign in the digital space into part of a study on building gender-based power in the digital space. Herein lies the importance of the definition provided by the United Nations Population Fund (UNFPA) in its 2021 advisory note on reporting digital violence: a practical reference guide for journalists and media outlets, which states: "Any act of violence committed by one or more individuals that stems from gender inequality and gender norms, and is committed, aided, aggravated, or amplified in part or entirely by the use of information and communication technologies or digital media, against a person based on their gender."



For these reasons, it is perhaps necessary to understand power relations and analyze their dynamics from a gender perspective for a more effective in-depth understanding of digital violence, that is, by transforming every action and every campaign into part of a study of gendered power construction in the digital space. Herein lies the importance of the definition provided by the United Nations Population Fund (UNFPA) in its 2021 “Reporting Tip sheet on Digital Violence: A practical reference guide for journalists and media”, which defines technology facilitated gender-based violence as: “An act of violence perpetrated by one or more individuals that is rooted in gender inequality and gendered norms and that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender”.

Digital violence includes cyberbullying, harassment, spreading misinformation, disinformation and mal-information. These behaviors require a comprehensive response including media and information literacy (MIL) education, content moderation, and reporting procedures. Schools and educational institutions must promote a culture of knowledge and respect, policymakers have a role to play in enacting legislation to address these issues and ensure perpetrators are held accountable, and tech companies have a responsibility to provide a safe online environment and a pathway to report any violence that may occur. These collaborative efforts from all parties are necessary for a safer and more inclusive digital world. This can help mitigate the harms of cyberbullying and promote respect for users around the world digitally.

Who Are the Victims of Digital Violence, and What Are Its Most Prevalent Types?

Both women and men can be victims of digital violence. However, statistics indicate that women and girls are particularly vulnerable to this type of violence . Not only are they more likely to be targeted by digital violence, they can suffer the effects and consequences that can lead to physical, psychological, and economic harm. Considering that knowledge is fundamentally important for individuals involved in social change, it is essential to learn how to analyze power dynamics to determine where intervention can be most effective. From this standpoint, developing an effective action plan and defining some manifestations of violent behaviors – whether directed at individuals, groups, or institutions – is a necessary research path.



Among the most prevalent types of digital violence, we mention the following:

Prevalent Types of Digital Violence

Cyberstalking

Cyberstalking involves persistent monitoring of a person's online activities in a manner that causes anxiety and fear, harassment, stalking, tracking, threatening and online controlling. An example issuing GPS phone tracking apps.

Sextortion

Sextortion is a form of coercion and corruption in order to extort sexual favors from the victim, which is sexual exploitation based on abuse of power. It occurs when someone threatens to distribute private and sensitive material using an electronic medium and can happen to anyone, especially women and children.

Image-Based Violence

Image-based violence A widespread and constantly evolving phenomenon of digital violence that includes various forms of distribution of images for the purpose of harm or misuse, as well as a means of obtaining image-based materials of other people with the help of digital technologies.

Examples include publishing nude photos without permission (also known as revenge porn) or receiving unsolicited sexual images.

Cyberbullying

The term bullying reflects aggressive behavior aimed at marginalization and harm. Here, network users are intentionally insulted, threatened, embarrassed, or harassed. It is a repeated aggressive behavior targeting individuals with the aim of harming them psychologically and socially. This negative behavior includes actions such as spreading rumors, threats, insults, embarrassment, and impersonation. These actions are committed across various digital platforms, from social media sites to photo and video sharing platforms. The dangers of cyberbullying are not limited to the victim but extend to society as a whole.



Cyber-Harassment

A form of cyber-violence and includes any persistent, repeated and extended behavior from outside the digital world such as excessive force towards victims through threats of violence, spreading defamatory lies that may cause embarrassment to the victim, and impersonating victims. Harassers may violate victims' privacy by posting sensitive information, such as nude photos or identification numbers, or harassers may use technology to disconnect from the internet. Cyber harassment often targets women and girls and is called "cyber violence against women and girls or cyber violence against women and girls as it occurs against young boys) which includes:

- Unsolicited emails or other messages of an explicit sexually nature;
- Offensive insinuations on social media and other platforms;
- Threats of physical or sexual violence;
- Hate speech meaning language that vilifies, demeans, threatens or targets an individual on the basis of their (gender) identity and/or other characteristics (such as sexual orientation or disability).

Cyber defamation and Online Blackmail

Cyber defamation and digital extortion: This type of violence can turn into sexual blackmail (blackmail through the threat of publishing private information, digital data, photos or videos that may be of a sexual nature); image-based abuse (non-consensual sharing of intimate images); defamation (using technology to disseminate private personal information and spread rumors or false information about them); and cyberbullying. It can turn into gender-based violence. It can be carried out by individuals or by digital mobbing gangs.

Online Hacking

This is the illegal intrusion into computer devices and networks with the aim of accessing, manipulating, or destroying sensitive information via the internet. This is carried out by an individual or a group of individuals with extensive experience in computer programs. Using auxiliary programs, they can access another computer and view its contents by exploiting vulnerabilities in security systems for unauthorized access to personal or private accounts and data. Hacking operations include a wide range of activities, such as identity theft, extortion, espionage, and the dissemination of malware.

Online Sexual Exploitation and Abuse of Children (OSEAC)

This term refers to the power of technology and its impact on a wide range of criminal acts that sexually target children through the use of information and communication technologies (ICTs), facilitating their full commission. These acts include, but are not limited to, the production, distribution, and possession of child sexual abuse material (CSAM), online grooming, sexual extortion of children, as well as their corruption and direct contact with children for sexual purposes. These criminal acts often take place online or via mobile devices, exploiting the trust and vulnerability of children, and leave deep and long-lasting psychological and social effects on the victims. The term "child sexual abuse material" refers to any material that visually depicts a child engaged in actual or simulated sexual conduct, or any depiction of a child's sexual organs for primarily sexual purposes, thereby reinforcing the long-term harmful impact of child abuse stemming from engaging children in sexual activities, whether through coercion, exploitation of a relationship of trust, or by targeting vulnerable children, including what may occur within the family, at school, or any other location, especially as technology contributes to the expansion of these crimes and facilitates their commission across geographical borders.



Online Hate Speech

on platforms is also considered a form of digital violence. Hate speech involves using digital platforms to disseminate or incite violence, discrimination, or hatred against individuals or groups based on characteristics such as race, religion, gender, and sexual orientation. This type of abuse can lead to psychological and physical harm, exclusion, as well as physical violence.

It is also important to be aware of deepfakes and their dangers. **Deepfakes** are AI generated and altered video or audio files disseminated in the digital space. These files have been manipulated using artificial intelligence, especially since they are easy to produce as algorithms in programs or applications allow for the creation of fake moving images, films, and audio recordings that are difficult to verify easily. This content can be used to spread digital violence.

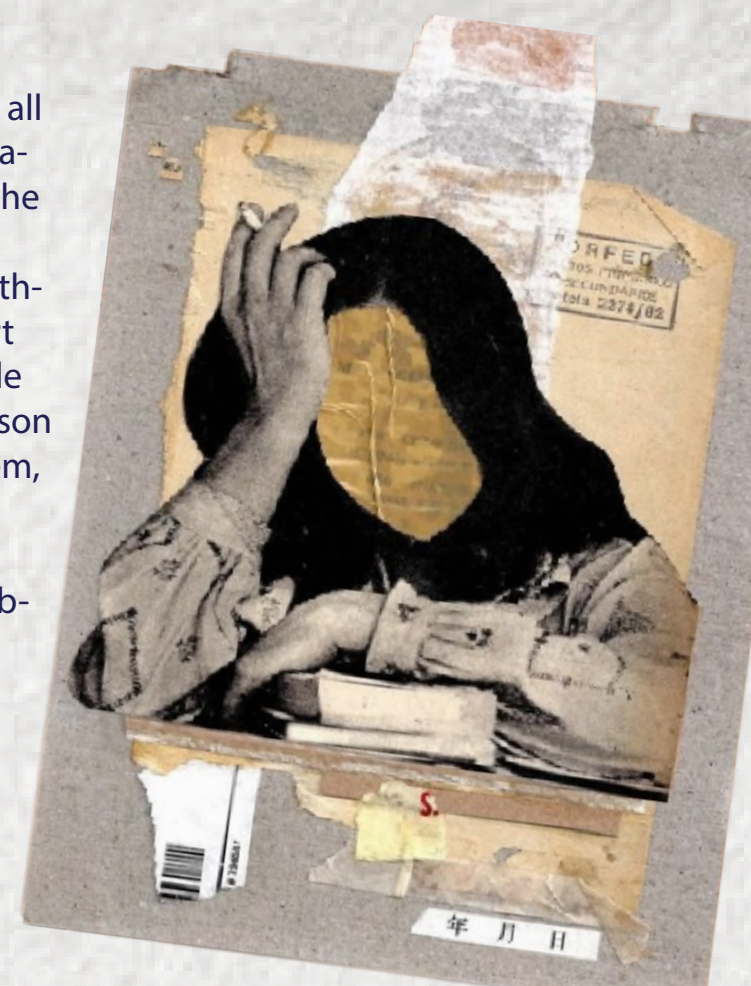
The term "Doxxing," is derived from the phrase "dropping dox (documents)," refers to the public dissemination of personal and private information without prior consent. This includes home addresses, phone numbers, email addresses, or financial details. This act can be a means of intimidation or to encourage others to harass the victim.

Mechanisms

A- Protecting victims by providing legal and psychological support, a safe and confidential mechanism for reporting digital violence crimes, and how to the protect marginalized groups. The roles of relevant authorities, including security institutions, the Ministry of Justice, the judiciary, the Ministry of Telecommunications (including the Telecommunications Regulatory Authority -TRA), the Ministry of Education, and any other concerned ministries or departments. Combating digital violence crimes requires a Multi-Stakeholder Governance Approach from all relevant actors, i.e. from the government to state institutions, the judiciary to technicians, as well as civil society organizations from educational institutions, to the individuals. The implementation of these proposals will build a strong protection system for victims of digital violence and foster a culture of cybersecurity and digital literacy for everyone, from all walks of life, social classes, and every resident in Lebanon. Stakeholders can work collectively to develop a comprehensive and decentralized process and protection mechanism for victims of digital violence, focusing on providing adequate support and facilitating easy and confidential reporting. This approach must also avoid victim-blaming, safeguard privacy, and address the full range of psychological and societal empowerment needs through the following:

1. A Comprehensive Mechanism to Protect Victims of Cybercrime in Lebanon

- Establishing laws and policies defining digital violence cases, and their degrees of severity.
- Establishing easy, clear, and confidential reporting mechanisms by building a . comprehensive protection system against digital violence. This includes clear government policies across all administrations and training trainers on how to receive and handle complaints, as well as supporting private initiatives within companies and especially in educational institutions.
- Build coalitions of judges and a committee of lawyers to provide legal aid and counseling, especially for those who do not have the financial means to do so This also includes include the Ministries of Justice, Telecommunications, Social Affairs, and companies.-Develop clear policies to protect personal data in the digital space, and regulate the collection, storage, and usage of such data.-Developing effective mechanisms for reporting digital violence crimes, ensuring the confidentiality of victims' data, providing them with the necessary support, and protecting whistleblowers in these cases.
- Providing psychological support through an alliance and developing binding laws for psychological follow-up for victims, while determining the cost and ensuring access for all targeted social groups, as well as determining the entity authorized to work on its activation, implementation, and review - Providing specialized hotlines that operate around the clock to offer initial support to victims.
- Providing free and specialized psychological and legal support services for victims whether they are children and adults. This can be achieved by establishing specialized support centers in all Lebanese regions. Providing secure and confidential online platforms to file reports, allowing victims to report crimes without having to go to police stations in person
- Organizing large-scale awareness programs about cybercrimes and how to prevent them, with a focus on vulnerable groups such as women, children, and the elderly.
- Whistleblower or witness protection programs implemented to protect the identity of victims who disclose what happened and may file a complaint or report and may be subject to retaliation.



2. A Comprehensive Mechanism to Strengthen the Capacities of Governmental, Security, and Judicial Institutions

- Training security and judicial personnel to effectively handle cybercrimes, including the collection and analysis of digital evidence, as well as a program for dealing with whistleblowers of violence and ensuring their protection.
- Enhancing regional and local cooperation to combat cross-border digital violence, and exchange specialized data based on the principles of transparency and the protection of personal data.
- Supporting non-governmental organizations (NGOs) working in field of combating digital violence, and enhance their role in raising awareness, and providing support to victims.
- Building partnerships with civil society organizations and international institutions to exchange expertise and knowledge, in the field of gender and cybercrime.

3. Protecting Vulnerable/Marginalized Groups

- Providing special protection for children by enforcing laws that criminalize the sexual exploitation of children online, and providing awareness programs for children and parents.
- Protecting women from cyber violence, such as harassment and sextortion, by providing them with legal and psychological support.
- Providing specialized support services for people with disabilities, who may be more susceptible to becoming victims of digital violence.

4. Legislative Amendments

- Modernizing Lebanese laws and activating their application according to technological developments to include digital violence and harmonize them with new developments.

5. Awareness and Community Consciousness

- The role of educational institutions through media and information literacy (MIL) programs.
- The role of media outlets by applying professional and ethical codes of conduct during coverage, away from leaks and without sharing names or information during investigations; as well as working on specialized content that encourages critical and lateral thinking without arousing feelings of fear or anger, i.e. content that helps avoid the risks of violence and provides pathways and mechanisms in case it occurs.
- Strengthening partnerships with civil society organizations to reach and support vulnerable groups effectively.

6. Economic Dimension

- Allocating a clear, transparent, and binding budget for the implementation of any of the proposals.
- Working with major platforms to allocate support from their advertising revenues across their pages to fund projects as part of their corporate social responsibility (CSR) fund.

7. Corporate Responsibility and Data Algorithms

Not long ago, social media users considered online platforms as empowering tools, spaces where citizens could express themselves freely, share ideas, and engage in unrestricted communication. However, over time, growing concerns have emerged regarding the role these platforms play, particularly in light of the vast amounts of personal data they collect and the algorithms they use. It is worth mentioning that these algorithms are sequential set of rules and calculations, social media platforms use to prioritize the content that users see on their pages. These rules are based on user behavior, content relevance, and post popularity within the local context of the content, and they differ from one platform to another. As such, these algorithms have a significant impact through the study of platform users' interaction with private data.

Therefore, today more than ever, major social media technology platforms must subject their algorithms to strict regulatory oversight to ensure that the rights of users and users globally are protected from any digital violence or incitement to hatred arising from social media algorithms that can become harmful based on the data collected by major tech companies. This model may generate financial profits for the companies, but the long-term consequences for human rights can be dire. Hence the call for transparency of the algorithms used to find, process, and present information and their underlying structure and procedures.

8. Artificial Intelligence (AI) and the Internet of Things (IoT)

- AI can help automate processes and improve the efficiency of IoT. These can learn from their environment and make decisions based on this learning, without human intervention. However, as these technologies advance, people are exposed to new forms of cybercrime, gender-based violence. Many cases of domestic violence are emerging through the use of IoT as a means of perpetrating it. The legal and normative frameworks for cybercrimes remain neutral towards specific forms of crimes committed online or forms facilitated by technology that affect everyone, including women .

9. Information Literacy

- Digital content is growing and big data is rapidly expanding and flowing at a rate that is unknown and unpredictable, yet its potential is worryingly imaginable. This development must be accompanied by basic strategies based on media and information literacy to understand not only what content is being consumed but also what is being produced, taking into account diversity, freedom, democracy, equality, gender equality and justice as well as local contexts.
- The skills are based on the following:
- Trainings on analyzing digital content to detect and scan for any violence within the content.
- Evaluating violent content that could potentially escalate into action;
- Creating content that offers an alternative to violence and makes a difference in providing useful information;
- Developing open educational resources (OER) tools and materials to help various entities integrate a gender perspective into their activities and enhance their participation in combating digital violence;
- Encouraging research and studies on the phenomenon of digital violence in Lebanon to better understand its dynamics and develop effective strategies to address it.

10. Information Disorder and its Impact on Fueling Hostile Discourse

- There are fundamental goals behind the principle of “Net Neutrality”, which is that the management of digital content must take into account, when developing digital platforms, creativity, freedom of expression, and the exchange of ideas, especially in light of information disorder or what is defined by misinformation, disinformation, and mal-information (MDM). All of these rely (intentionally or unintentionally) on unverified information and can contribute to the spread of incorrect concepts, potentially leading to hate speech, the impact of which we witness during crises and in the dynamics of conflicts, situations of violence, and work on humanitarian issues. We cannot forget the opportunities arising from the rapid development of digital information technology. However, online communication studies indicate the interaction of hate speech and information disorder with dehumanizing language and imagery, supported by rapid dissemination algorithms. Therefore, there is a necessity to work on big data, human rights, and trust.
- Finally, this research emphasizes the importance of dealing with the phenomenon of digital violence seriously and effectively, through the concerted efforts of all concerned parties. It underscores the need to enact a comprehensive law to combat this phenomenon, taking into account gender and intersectional specificity, and providing the necessary protection for victims.
- It also provides practical recommendations to ensure the effective integration of the principles of justice and equality based on gender, such that cybercrimes are addressed in a way that protects fundamental rights, while ensuring the transparency of negotiations and the participation of human rights organizations and women's rights organizations. It also emphasizes the need to consider the rights of all groups, including persons with disabilities, persons with limited income, and various other social groups, in all activities related to combating digital violence. All of the above is based on the study of existing project models and international resources and references.