Digital Violence Against Women in Jordan: Legal and Institutional Context

Feb
2024

Esraa Mahadin
Hussein Suraireh
Dr. Nadia Al-Sakkaf

IDRC · CRDI
Canada

secdev.foundation

@سلامة

Acknowledgments

Research team

Esraa Mahadin is a legal consultant and attorney specializing in gender-based violence. She serves as the Executive Director of the Qalat Al-Karak Center for Consultations and Training.

Hussein Suraireh is an engineer specialized in sustainable & equitable communication and digital security. He serves as a policy and legislative analyst for governmental and non-governmental organizations.

Dr. Nadia Al-Sakkaf 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.

Editorial team

Judge Anwar Mansouri (legal editor) 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.

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 Ala Elfellah, Osama Moussa, Jesus Rivera and John Hall.

The SecDev Foundation

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. 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 against women across the MENA region. Responsibility for any views expressed in these studies rests with the authors.

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

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

Abstract

This study examines the reality of legal texts pertaining to how cybercrimes against women are addressed in Jordan. It further surveys the legal and institutional framework associated with digital violence in Jordan by reviewing international treaties ratified by the Jordanian government as well as national legislation used to prosecute digital crimes, along with legal principles in this field.

It also provides the input of experts and direct stakeholders, such as judges, attorneys, and security personnel, who discussed the difficulties of addressing gender-based digital violence in the absence of specialized legal texts and provided recommendations concerning this issue. It concludes that in the absence of specific and clear provisions in the legislative and legal system to protect women from gender-based digital violence, legislators and judges can rely on equality and protection principles in constitutional jurisprudence as well as relevant provisions in various laws to criminalize digital violence against women. In addition, national policies and international treaties ratified by Jordan play a crucial role in addressing this issue.

This study recommends amending various legal frameworks, including digital crime laws, by adopting a gender-sensitive approach and establishing institutional procedures for stakeholders involved in combating digital violence against women in Jordan.

Contents

Executive Summary

The primary objective of this study is to investigate the reality of legal texts and how they handle cybercrimes against women in Jordan. To this end, this study examines the pertinent provisions in the Jordanian constitution, international treaties ratified by the Jordanian government, and national legislation and laws implemented by the Jordanian judiciary in prosecuting digital crimes. Additionally, the research delves into local and regional studies and statistics on the issue, as well as the testimonies of specialists, judges, and attorneys regarding the challenges of addressing gender-based digital violence in the absence of specialized legal texts. Finally, the study offers recommendations for utilizing current constitutional principles and the legislative system to support judicial procedures that protect women in the digital realm and hold perpetrators accountable while awaiting the enactment of specialized legislation.

In doing so, legal arguments for the necessity of advocating a special legal text to combat cybercrimes targeting women in Jordan were presented. This study adopts an analytical legal approach by examining legal texts related to cybercrimes in general and violence against women in Jordan. It conducts this analysis from a human rights perspective and examines the institutional context in which the cybercrime unit operates. The study also employs a descriptive method, collecting and analyzing previous studies and testimonials from seven interviewees with specialists in the field of combating cybercrimes.[1]

The study highlights that the absence of a clear legal text criminalizing violence against women in the digital realm represents an obstacle to safeguarding women in cyberspace and contributes to the persistence of perpetrators. Nevertheless, considering the current legal system, this research argues that the legislator can enact legal adaptation and suspicion regulations using the existing legal framework, including the fundamental laws related to combating various forms of violence against women in Jordan, such as Penal Code, No. (16) of 1960 with amendments, Jordanian Civil Law, No. (43) of 1976, the Protection from Domestic Violence Law, No. (15) of 2017, the Anti-Trafficking Law, No. (9) of 2009, Personal Status Law, No. (15) of 2019, Electronic Transactions Law, No. (15) of 2015, and Cybercrime Law, No. (17) of 2023, as well as the constitutional principles and relevant international treaties ratified by the Hashemite Kingdom of Jordan.

It is crucial for relevant authorities to understand the legal gaps and provisions that allow them to apply constitutional principles and analogies to criminalize digital violence against women in anticipation of drafting specific legislation.

Through the examination of the connections between digital violence against women and the legal system, it was discovered that the process begins with the victim filing a complaint, either at a police station or through the cybercrime unit located in every major police directorate. The complaint is then transferred to public prosecution, which directs the cybercrime unit to investigate the case technically and criminally. This enables the public prosecutor to present the appropriate legal adaptation and suspicion regulations to the misdemeanor court, which issues punitive judgments carried out by relevant security agencies. In some cases, technical implementation may be required by the cybercrime unit, such as by blocking websites.

[1] In the appendix is a list of references and experts who were interviewed.

The cybercrime unit has been mandated by public prosecutions to systematically monitor and pursue organized cybercrimes that target Jordanian residents both within and outside the country. This is done in close coordination with local and international authorities. In addition, the unit is responsible for tracking the latest trends and the sophisticated forms of these crimes.

Since its establishment in 2008, this unit has faced a scarcity of resources and requires additional support from the governorate and the main center to accommodate the increasing flow of complaints and cases. It is essential to train those responsible for this unit and the various judicial and prosecutorial bodies in cases of digital violence against women, due to its specific nature and severe consequences.

Coordination between the aforementioned unit and civil society institutions is also necessary, especially in relation to the psychological and social dimensions of digital violence against women. This type of crime is similar to domestic violence and requires specific procedures within the family protection system such as psychological care, shelter, and custody. Therefore, it is essential for the public prosecutor and judges to treat cases of digital violence against women as domestic violence.

Legally, gender-based digital violence exceeds the private family space, as the Internet is considered a public domain. Nevertheless, given that this type of digital crime specifically targets women and resembles domestic violence, it has been subjected to the same procedures for psychological and shelter protection.

This study indicates that telecommunications firms operating in Jordan are not legally bound to address grievances concerning misuse. Instead, they present themselves as facilitators of communication and provide essential information to judicial authorities, when necessary, without assuming an executive role in safeguarding or preventing violations through their networks. Consequently, they can utilize their capabilities within the ambit of criminal investigations of these crimes to enable the judiciary to procure potential digital evidence.

A source in the cybercrime unit argues that although cybercrimes against individuals tend to focus on women,[2] published reports and data do not provide a clear picture of digital crimes by gender and, importantly, by motive. This is because women, like men, are susceptible to various cybercrimes, such as bank data theft or information system sabotage, regardless of the victim's gender. Thus, it is not sufficient to consider only the gender of the victims. Nevertheless, this study recommends incorporating a gender approach in the statistics or creating a special table for women as victims of cybercrimes, including the type of crime and its association with the motive, to distinguish gender-based crimes that affect women simply because they are women from other crimes.

The absence of these details makes it difficult to measure the problem and design effective solutions, such as developing comprehensive strategies for deterrence, prevention, punishment of perpetrators, and compensation for victims.

This study revealed a noticeable deficiency in societal knowledge concerning digital violence among both women and policymakers responsible for such crimes. While there is a set of legislation and procedures, despite their limitations, women can resort to when they are exposed to digital violence in Jordan, as detailed in this research, due to the lack of awareness of these legal resources and the necessary qualified personnel to address these cases. Consequently, they tend to avoid official channels to report such incidents, leaving them feeling unsafe and unsupported. Therefore, the significance of

[2] Statements by the Director of the Cybercrime Unit, Major Mahmoud Almaghayrah, to the Arabic Independent in the report published in August 2022.

cybercrime law lies in the fact that it affects all individuals directly and personally. This is because the likelihood of becoming a victim or perpetrator of such a crime increases with the growing reliance on electronic means of communication in daily life, which has become prevalent. Moreover, cybercrimes are new and virtual in nature, and as such, society may not consider them genuine. However, it is important to note that legally, ignorance is not a valid excuse that protects both parties from crime.[3]

Violence on the Internet, like other forms of violence, continues to be under-reported. This is evidenced by the testimonies collected for this study, which indicate that the seriousness of addressing digital violence against women in Jordan is inadequate. This is troubling, as the rate of this phenomenon is increasing, and the potential for digital violence to escalate into real-world crimes is even more concerning. There have been numerous instances where digital violence has led to actual crimes and threats made on social media have been carried out in the real world.

This study found that Jordanian legal texts generally fall short of effectively addressing gender-based cybercrimes. In particular, there are inadequacies in defining these crimes and their corresponding penalties. The Jordanian judiciary encounters challenges in applying the current laws to these crimes because of the absence of clear legal definitions and specialized centers for dealing with them. Moreover, there is a scarcity of prevailing customs, awareness of ways to implement legal adaptation, and a list of suspicions to support women.[4]

Despite the enactment of the Cybercrime Law, No. (17) of 2023, published in the Official Gazette on August 13, 2023,[5] it does not provide special provisions that address the unique nature of digital violence against women. The law does not address the two dichotomies of freedom and protection that are essential to preserving women's right to express their opinions and to engage in digital activities within the bounds of the law that safeguard them from violence and ensure their privacy, which is often compromised by various forms of cybercrimes.

The experts' testimonies obtained in this research suggest that digital violence against women exacerbates the digital divide and can hinder access to essential services, such as distance education and legal support. Therefore, it is crucial to carefully monitor the post-pandemic effects of cyberviolence. It is important to note that online and offline violence are interconnected, making it difficult to differentiate between actions that originate in digital environments and those that occur outside of them.

Drawing on the outcomes of this research, a set of recommendations was formulated,[6] with the foremost being the need for the Jordanian legislature to issue a specific legal text targeting gender-based cybercrimes. This could be accomplished either through individual law or as part of the Cybercrime Law 2023. Such a legal framework aims to curtail and mandate the prevention of digital violence against women, providing a clear definition of the meaning of digital violence against women. This measure is essential for bridging the existing legal gap in this area, thereby ensuring the safety of women against these crimes.[7]

[3] Quoted from a description of one of the beneficiaries of the Karak Castle Centre's specialized digital safety awareness campaigns.

[4] Khaled Al-Qudah- digital media expert, member of the Jordanian Journalists Syndicate.

[5] Official Gazette, Issue No. 5874, published on August 13, 2023.

[6] The study presents a number of detailed recommendations in the recommendations section in the conclusion of this research.

[7] Attorney Nidaa Al-Shuwaikh.

The government of Jordan is responsible for evaluating the existing legal framework for cybercrimes, such as the Penal Code and Communications Law, and ensuring that it includes provisions to criminalize gender-based cybercrimes and increase penalties for such offenses. This is in line with the National Strategy for Women in Jordan.[8]

The need for periodic reviews arises because the nature of technology-related violence is continually evolving, leading to changes in its definition and criminal application. Consequently, it is necessary for lawmakers to regularly update regulations governing these digital spaces to ensure that they remain a haven for free expression, where women can seek refuge in the event of any violation.

The primary recommendations of this study are the encouragement of judges, attorneys, and public prosecutors to utilize existing legal principles and texts to safeguard women in the digital realm through constitutional provisions that guarantee gender equality and the principle of protection, as well as communication laws and certain sections of the Penal Code. These legal provisions enable the legislator to make necessary adjustments to protect women and criminalize digital violence against them in Jordan. This adjustment includes leveraging the second objective of Jordan's National Strategy for Women 2020-2025, which pertains to all forms of gender-based violence, as well as the fourth objective that focuses on institutions and policies that align with the strategy's goals.

This study emphasizes the importance of providing appropriate training for public prosecution, the judiciary, and security agencies to humanize this form of legal case and understand its nature. These crimes have deeper social and psychological dimensions than other digital crimes; therefore, specialized training is necessary to address digital violence against women. Additionally, there is a need to collaborate with entities that provide government services and coordinate with stakeholders, particularly judicial police and civil society organizations, to develop targeted services for female Internet users. This study also recommends involving all relevant parties and institutions, including telecommunications companies and Internet service providers, to facilitate reporting mechanisms and coordinate with security and judicial authorities to combat digital violence against women. It is also essential to launch community awareness campaigns about the risks of gender-based cybercrimes and their legal consequences, as well as to provide information on how to prevent and report these violations. This study underscores the need for programs, policies, and legislation that raise awareness of the dangers of cybercrimes against women and provides guidance on how to confront them. It is crucial to hold perpetrators accountable and provide compensation for victims, as outlined in the Penal Code (Articles 42 and 43) and Civil Law (Articles 266 and 267).[9]

It is essential to inform Internet users about the protocols and locations for reporting cases of violence against women facilitated by information and communication technologies, whether the offensive is on the ground or on social media platforms, such as reporting mechanisms of offensive content on Facebook.

Moreover, enhancing the capabilities of justice elements and police specializing in combating Internet-based violence is necessary. Internet intermediaries should establish clear and high-level commitments to support women's safety online and provide easy and transparent procedures for reporting and

[8] National Strategy for Women in Jordan, 2022.

[9] For example, the Jordanian Court of Cassation stated in a ruling: *"Assessing compensation for moral damage resulting from the crime of corrupting the marital bond, which led to harming reputation and honor, does not violate the law and is one of the factual matters in which the trial court is independent."*

submitting complaints regarding digital violence, including on social media and through hotlines and services suitable for minors.

In this regard, it is important for the Cybercrime Unit to receive adequate support, including the provision of qualified and specialized human resources, sustainability of expertise in the unit, and development of communication policies and mechanisms between the unit and other concerned government agencies. It is also essential to establish a specialized joint committee to address gender-based digital violence, comprising representatives from the Cybercrime Unit, judiciary, Ministry of Digital Economy and Entrepreneurship (previously known as the Ministry of Communications and Information Technology), Telecommunications Regulatory Authority, National Center for Human Rights (an autonomous institution by special law), National Committee for Women's Affairs (a specialized civil society organization), and attorneys from civil society and the Jordanian Lawyers Syndicate. This committee should facilitate cooperative efforts between these entities at the case level and emphasize the human dimension of these cases rather than focusing solely on plans, policies, and general frameworks. Furthermore, the development of a protection system and reports that guarantee a fair trial for crimes of high specificity, which resembles domestic violence, has a significant impact on victims.

Investment and cooperation with technology companies advocating for women and civil society organizations should continue to develop short-, medium-, and long-term solutions. The newly proposed law suggests the opening of representative offices for any platform, followed by more than 100,000 individuals residing in Jordan. This policy aims to prevent these platforms from monopolizing their own policies in this context and obliging them to apply security recommendations locally. This proposal aligns with the recommendations of the Arab Convention for Combating Cybercrime and Council of Arab Information Ministers.

According to the research findings, it is essential for the Public Security Directorate to release criminal statistical data categorized by gender for all relevant crimes. Additionally, an annual criminal report should provide more detailed information about such crimes, which will facilitate an accurate diagnosis of the form of criminal development and its current status. This information can be used by concerned parties, both locally and internationally, to conduct more research and share data, which is crucial for identifying and addressing crimes that transcend cultural and geographical boundaries. By adopting a rights-based approach, it is possible to develop effective mechanisms to confront such crimes.

The digital realm, particularly social media platforms that are notorious for the prevalence of violence against women, can also serve as a means to disseminate awareness campaigns aimed at eradicating and eliminating all forms of violence directed against women. It is the responsibility of human rights and justice workers, as well as defenders of women's rights, to actively participate in these digital campaigns, as past experiences have demonstrated their efficacy in several Arab countries such as Tunisia, which boasts an advanced legal framework to protect women.[10]

[10] Anwar Mansri and Shaima Riahi, The reality of legal texts and the legal and institutional response to digital violence against women in Tunisia, SecDev Foundation and Salama Program.

Context of Digital Violence Against Women in Jordan

In 1993, the United Nations General Assembly passed the Universal Declaration on the Elimination of Violence against Women. The declaration defined violence against women as "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." It is worth noting that violence against women is a prevalent violation of human rights worldwide.

Digital violence against women in virtual and diverse digital spaces is a continuation and reinforcement of real-world violence directed towards women, in which societal beliefs are projected onto digital interactions. The root cause of this issue lies in the social environment and traditional gender stereotypes that perpetuate the belittling view of women through confrontational discourse and negative discrimination. Unfortunately, many do not view digital violence as harmful and do not classify it as violence, making it difficult for those who recognize it as violence to speak out without facing bullying and violent discourse.[11]

Despite its many advantages, modern technology has contributed to the emergence of new forms of violence against women, with stalking and electronic pursuits, bullying behaviors, and defamation campaigns being among the most prevalent. Additionally, there is electronic blackmail, electronic sexual harassment, surveillance and spying through computers, illegal use of technology and the Internet for images and video clips and altering them for illegal sexual purposes and human trafficking, impersonating names and fictitious personalities to entrap women and girls, particularly through applications with chat features, threatening violence and physical safety, as well as a multitude of other physical, moral, and psychological threats. It is essential to recognize and address these issues to protect women's well-being in the digital age.

Accordingly, this study utilizes the United Nations' definition of technology-facilitated gender-based violence, which "is any act that is committed or amplified using digital tools or technologies causing physical, sexual, psychological, social, political, or economic harm to women and girls because of their gender."[12]

The seriousness of digital violence, which is a spectrum of the broader category of cybercrimes, is compounded by the fact that it encompasses a vast domain, namely the Internet. If privacy is breached, private information about women is disclosed, or any form of digital violence occurs, it becomes difficult to regulate or mitigate the damage. This problem is further exacerbated when the victim's profession requires her to be in the public eye, as in the case of professionals such as attornys, journalists, politicians, or doctors.[13]

Despite the pervasiveness of this phenomenon in the Arab world, the legal system in most Arab countries still disregards its significance in their legal requirements. Even when acknowledged, the seriousness of addressing it is inadequate, as evidenced by the increase in its occurrence. Even more

[11] Khaled Al-Qudah- digital media expert and member of the Jordanian Journalists Syndicate, Karak Castle Center for Consulting and Training's study on digital violence against women.

[12] UN Women – Headquarters. Frequently asked questions: Tech-facilitated gender-based violence

[13] Khaled Al-Qudah- digital media expert, member of the Jordanian Journalists Syndicate.

concerning is the transition from digital to real violence, which has resulted in numerous cases of digital violence being carried out as crimes. There are also numerous stories of financial blackmail and threats that originate from online relationships.[14] This highlights the need for laws to specifically address such crimes and protect personal rights, as digital threats can have both real and criminal consequences. Local authorities must take immediate action against the threat, treating it as a violation of community peace and breach of public rights. It is also the responsibility of those who use social media to promptly report cases that pose a genuine threat to public safety, in addition to reporting to the electronic help center of the application.

Although Morocco and Tunisia have adopted a comprehensive approach to address the issue of violence against women, the rest of the countries in the region have laws that criminalize such acts scattered across many legal frameworks, such as the Penal Code, Family Laws, and special laws. However, there are no specific laws in Jordan that address violence against women.

Researchers indicate that digital violence is more pernicious than physical violence because it is difficult to escape, as it has become an integral part of daily activities, such as education, services, and public relations. Furthermore, the scope of the potential audience and anonymity of the perpetrators make it more insidious.[15] Digital violence against women also has a marginalizing effect on their role in society. Additionally, it weakens them economically and politically, as some women may withdraw from the public space, either as candidates or voters, due to reluctance to participate in elections.[16]

A study conducted by the Jordanian National Committee for Women's Affairs on violence against women in the public and political sectors revealed that 65% of working women had encountered violence in public life.[17]

According to the respondents, psychological and moral violence were the most prevalent forms of violence, with 90% having experienced it, followed by verbal abuse at 69%. Additionally, 63% of respondents reported being subjected to digital violence and bullying, while 18% experienced sexual violence or harassment. The study showed that technology and social media platforms were the most commonly used means of perpetrating violence, with 55% of respondents confirming that they were victimized using these platforms.

Verbal violence is a significant problem for women in the Arab world and Jordan in particular,[18] and unfortunately, it also prevails in digital spaces. According to official data[19] from human rights organizations[20] that work in this field, especially because the number of victims of digital violence is increasing, their forms on the Internet, particularly on social media platforms, are manifold.

Considering the aforementioned information, digital violence can be considered one of the most challenging, dangerous, and threatening types of violence to society, as it affects the social and

[14] Examples can be found in this report.

[15] Khaled Al-Qudah- digital media expert and member of the Jordanian Journalists Syndicate, Karak Castle Center for Consulting and Training's study on digital violence against women.

[16] Dr. Muhammad Miqdadi, Secretary-General of the National Council for Family Affairs. You can also refer to the Karak Castle Center for Counseling and Training, Violence against women in the parliamentary elections in Jordan, 2020.

[17] National Committee for Women's Affairs. Study of violence against women in the public and political spheres in Jordan, 2022.

[18] Challenges of creating Arabic digital content, Dr. Mahmoud Abu Farwa Al-Rajabi, 2023.

[19] Cybercrime Unit- Public Security Directorate, Jordan, 2022.

[20] Digital electoral violence against women in Jordan, Karak Castle Center for Consulting and Training, 2022.

psychological lives of individuals, which may lead them to engage in criminal activities that threaten the stability of society.[21]

Exposure to digital violence increased during the COVID-19 pandemic, which exacerbated the costs of the hidden pandemic represented by violence against women, particularly in light of the ongoing crisis and the inevitable shift to the digital space. The United Nations Women's Agency's regional office in Arab countries conducted an online survey in nine countries (Morocco, Libya, Tunisia, Jordan, Palestine, Lebanon, Iraq, and Yemen) in 2022 to shed light on the increase in cases of violence during the pandemic and actions taken towards violence.

The results showed that digital violence was the most reported form of violence during the first months of the pandemic, with Iraqi women having the highest rate of exposure to digital violence at 70%, followed by Yemeni women (62%) and Jordanian women (60%).[22]

The study indicated that 16% of the women in the Arab region were subjected to digital violence. This percentage may be low due to reluctance to report, as among the respondents who reported being subjected to violence, only 60% did so.[23]

Drawing from a comprehensive study conducted by the National Committee for Women's Affairs in 2022, it is evident that digital violence is the most prevalent form of aggression faced by prominent women in the public domain. This trend can be primarily attributed to widespread and convenient access to technological resources.[24] The study revealed that a substantial majority of the respondents (63%) were subjected to digital violence and bullying. This constitutes the third most common type of violence, followed by psychological and moral violence (90%), and verbal abuse (69%). It is essential to recognize that digital violence against women manifests in various guises, ranging from the dissemination of sensitive personal information to sexual blackmail, phishing, bullying, stalking, harassment, and revenge through the publication of intimate photographs.

Forms and Dimensions of Digital Violence Against Women

The United Nations Entity for Gender Equality and the Empowerment of Women, known as UN Women, categorizes digital violence against women into six distinct forms based on the manner in which the offense is committed. The six forms are as follows:

1. **Hacking:** This refers to the unauthorized or illegal use of technology to access a woman's devices and accounts to obtain personal information or to modify or defame her reputation.
2. **Impersonation** involves the use of technology to assume the identity of a victim or another person to access private information, embarrass the victim, or create forged identity documents.
3. **Stalking:** This involves the use of technology to track and monitor the activities and behaviors of a victim, either in real time or in the past.

[21] Abdul Mahmoud; Abbas Abu Shama. human; Muhammad Al-Amin. (2005). Domestic violence in the light of globalization. (First edition). Riyadh- Saudi Arabia: Center for Studies and Research; Naif Arab University for Security Sciences. | Hilaal; Naji Muhammad. (2007). Domestic violence in Emirati society: A field study. (First edition). Sharjah- United Arab Emirates: Police Research Center; Sharjah Police. | Ihab Al-Hadary (2010). Alternative Space, Political and Social Practices of Arab Youth on the Internet, Center for Arab Civilization, Giza.

[22] UN Women. Violence against women in the digital space: Insights from a multi-country study in Arab countries, 2022.

[23] UN Women. Violence against women in the digital space: Insights from a multi-country study in Arab countries, 2022.

[24] National Committee for Women's Affairs. Study of violence against women in the public and political spheres in Jordan, 2022.

4. **Harassment:** This involves the repeated use of technology to contact, annoy, harass, and threaten a victim through continuous calls, text messages, voicemails, or emails, and may also involve threats or blackmail.
5. **Recruitment:** This involves the use of technology to attract potential victims of violence, such as through fraudulent job advertisements on social networking or job sites.
6. **Distributing Disturbing Materials:** This involves the use of technology to process and distribute defamatory and illegal materials related to the victim.

It is worth noting that the Jordanian Cybercrime Law encompasses all of these forms of cybercrime, but treats them in a neutral manner, without specifying the nature of the crimes when the victim is female, and violence is gender-based. This lack of differentiation is viewed as a deficiency in the law and presents an opportunity for the legislature to amend the law to better protect women until a comprehensive legal text is enacted that explicitly criminalizes violence based on social type.

Advancements in technology have brought about several characteristics of digital violence that have a greater impact on female victims than other forms of violence. These characteristics can be summarized as follows:[25]

- **Digital violence against women is far more serious in its consequences than traditional or physical violence:** Cybercrimes involve the ability to conceal one's true identity, making it difficult to determine the extent of harm inflicted on the victim. In some cases, fear of stigma, discrimination, or defamation may cause victims, particularly females, to resort to suicide.
- **Digital violence against women is transboundary and global in nature:** This type of violence is not confined to specific time or location constraints. Furthermore, technological advancements have enabled the expansion of violent, aggressive, and illegal practices, which can occur at any time and transcend geographical and temporal limitations without constraints.
- **Digital violence is constantly evolving and developing:** It continuously develops with the advancement of modern technological methods that enable the long-lasting impact of such violence. In many cases, this type of violence is ongoing, such as instances of defamation and slander. However, effective controls and technical interventions can end these crimes.
- **Easy occurrence and fast proliferation:** The ease with which this form of content can be accessed and disseminated is a major concern because once it is published online, it is often impossible to prevent its dissemination.
- **It lacks physical interaction:** The communicating parties, comprised of the perpetrator and the victim, do not engage in any physical interaction, and this form of communication is less taxing than traditional violence as it relies on mental and intellectual prowess rather than physical strength.
- **It is easy to contact victims who lack the ability to defend themselves:** Social media has allowed perpetrators to contact victims at any time and location, while simultaneously rendering the victim's self-defense or evasion of such violence exceedingly challenging for a multitude of reasons, including insufficient knowledge of self-protection techniques in such situations, inadequate comprehension of the law, or apprehension of societal stigma. Consequently, victims are often inclined to remain silent.

[25] UN Women. Violence against women in the digital space: Insights from a multi-country study in Arab countries, 2022.

The impact of digital violence on women is particularly pernicious, and often surpasses the negative consequences of traditional forms of violence:[26]

- **Psychological consequences:** The consequences of digital violence can be severe for women, leading to various psychological consequences including depression, isolation, and stigma, as well as the possibility of resorting to suicide.
- **Social consequences:** Victims' families typically avoid disclosing the cybercrimes to which their daughters are subjected because of the fear of societal judgment and suspicion of the behavior of these girls. They opt for silence, feel socially oppressed, and are unable to hold the offenders accountable for their actions, which exacerbates their sense of anger. Such societies, especially those in conservative Arab cultures, can also resort to physical violence against the victim when the family discovers the digital defamation or insult inflicted on her.
- **Economic consequences:** Digital violence and defamation can have serious economic repercussions for victims, including potential loss of employment opportunities and earning potential. If the victim is a woman who supports her family, the situation becomes even more dire. Her exposure to this type of crime and her inability to defend herself can make it difficult for the family to maintain economic independence and stability, having a ripple effect on the wider community and society.[27] Even if a woman does not directly contribute to her family's finances, her economic independence remains an important factor in maintaining her overall rights and freedoms.

Although UN Women have recognized and addressed these three consequences, there are other significant consequences of digital violence against women that must also be considered. For example, political consequences can limit women's participation in the political sphere. Additionally, indirect consequences may arise from the escalation of violence, leading to potential physical harm or even loss of life in severe cases.

[26] UN Women. Violence against women in the digital space: Insights from a multi-country study in Arab countries, 2022.

[27] Khaled Al-Qudah- digital media expert, member of the Jordanian Journalists Syndicate.

Feasibility and Methodology of the Study

As noted earlier, digital violence against women has gained prominence in Jordan, just as it has in many other countries worldwide. However, it is disappointing that legal and legislative frameworks do not address this type of violence. Therefore, this research is seen as laying the groundwork for advocacy efforts aimed at both the legal and human rights levels, with the primary objective of initiating the process of drafting regulating laws. This can be achieved through a comprehensive review of the legal and institutional frameworks governing digital violence against women in Jordan. This review aims to offer comprehensive insight into the legal and institutional landscape surrounding digital violence against women in Jordan. Furthermore, it provides recommendations that encompass the legal adaptation of existing measures and the creation of new laws that would criminalize digital violence against women. Additionally, this review proposes the establishment of deterrent mechanisms and empowerment strategies for women, including appropriate compensation.

This research team began with a comprehensive review of pertinent studies to understand the extent of digital violence in Jordan. This was followed by an investigation of the regulatory legal frameworks, encompassing the Jordanian constitution, international treaties and covenants, relevant laws such as the Cybercrime Law for 2023, and concluding with national strategies and policies pertaining to this topic.

The legal framework safeguarding women from all forms of violence in Jordan is composed of several key laws, including Penal Code, No. (16) of 1960 with amendments, Jordanian Civil Law, No. (43) of 1967, the Protection from Domestic Violence Law, No. (15) of 2017, Electronic Transactions Law, No. (15) of 2015, the Anti-Human Trafficking Law, No. (9) of 2009, Personal Status Law, No. (15) of 2019, and Cybercrimes Law, No. (17) of 2023.

In addition to the expertise of the specialized research team, this study sought the input of seven legal experts and professionals in judicial and human rights. These interviews served to present the results of this study and incorporate practical feedback and recommendations.

Although this research is unprecedented, it is considered the initial step in an ongoing research journey. This is due to the association between this type of violence and rapidly evolving technology and the need to stay abreast of the potential consequences of these changes through regular review. The ultimate goal was to make the digital world a safe space for women in Jordan.

National and International Legal Frameworks Related to DVAW

Until recently, legislative, executive, and judicial authorities have employed distinct strategies in the realm of Internet legislation. Most nations regulate the Internet in accordance with their own political, legal, ethical, and cultural values. However, owing to the global nature of information and communication technology development, which transcends the control of individual countries, the establishment and implementation of effective cybercrime legislation presents a significant obstacle for countries with these three authorities. As a result, cybercrimes pose a significant challenge to legal bodies, whether in developed or developing countries, because the legislative process tends to be slow and unable to keep pace with the rapid evolution of cybercrimes.

Over the past two decades, discussions on women's issues and their empowerment have persisted in Jordan at various levels. Although some tangible outcomes have emerged from these discussions, there are instances where the results remain theoretical. For example, the government established the Jordanian National Committee for Women's Affairs and allocated seats to women in the Jordanian House of Representatives through the quota system. Moreover, several government strategies have emphasized the importance of empowering women. However, Jordanian laws related to gender-based digital violence often fall short in protecting women, who are the most affected group. Such legislation does not adequately consider the specific local social realities and long-term consequences of systematically marginalizing women's roles. Therefore, it is crucial to examine the relationship between legislation and societal factors including customs, traditions, and norms. This section provides an overview of significant local and international laws and agreements related to digital violence against women in Jordan, both directly and indirectly.

The examination of these texts was conducted by considering six essential principles that any legislation ought to have with the intention of bolstering safeguards for women who are subjected to the consequences of digital violence more broadly. The principles are as follows:[28]

1. **Ensuring Comprehensiveness:** The legal text should incorporate all forms of harm, violence, and threats that may affect the lives and rights of women within the digital space.
2. **Protecting Victims:** Effective protection should be provided for women victims of digital violence, ensuring their safety and the safety of those who report crimes, as well as safeguarding them from any potential danger.
3. **Tightening Penalties:** Penalties imposed on perpetrators of cybercrimes targeting women should be increased, taking into account their exploitation of the vulnerability of victims and their inability to protect themselves. No exceptions should be made for relatives of victims involved in crimes who may benefit from mitigating excuse for punishment.[29]
4. **Confidentiality and Privacy:** These issues should be handled with confidentiality and respect for privacy, given the social sensitivity of these matters and their impact on the status, reputation, and dignity of victims.

[28] Attorney Nidaa Al-Shuwaikh and Attorney Muhammad Abu Zannad- member of the Bar Association Council.

[29] Article 98 of the Penal Code deals with the principle that outbursts of anger give an excuse to perpetrators of crimes related to honor regarding female relatives. However, this principle was canceled in 2017 when Article 340 regarding honor killings was amended and limited to the crime of murder, with equal excuses for both genders. In order not to leave room for the return of honor killings as a result of digital violence, the importance of not making exceptions was highlighted.

5. **Developing Litigation Mechanisms:** Specialized litigation mechanisms should be established to handle similar cases, and the principles of fair arbitration should be included in these processes, taking into account the specificity of the impact of these issues on women.
6. **Abolishing Inappropriate Articles:** Laws that allow for the reduction of personal rights and criminal penalties that could mitigate penalties for perpetrators of crimes should be abolished.

The Jordanian Constitution

The Constitution serves as the highest authority in the Jordanian legal system and is the primary source for developing laws related to the roles, rights, and obligations of Jordanian women. Article 6, paragraph 1, states the following:

> *"Jordanians are equal before the law with no discrimination between them in rights and duties, even if they differ in race, language, or religion."*

Following constitutional amendments in 2022, the right section of the Jordanian Constitution was amended to include the term "Jordanian women" alongside “Jordanian men” in the title of the second chapter, which pertains to rights and duties. This change resulted in the title of the chapter becoming "Rights of Jordanian Men and Women and Their Duties," as the state moved to modernize the political system, which paved the way for the inclusion of the sixth paragraph in Article 6, which states:

> *"The state guarantees the empowerment of women and supports them to play an active role in building society, ensuring equal opportunities on the basis of justice and fairness, and protecting them from all forms of violence and discrimination."*

The Jordanian Constitution, which was first introduced in 1952, has consistently demonstrated a forward-thinking approach to the principles of freedom and protection. In multiple provisions, the Jordanian constitution explicitly affirms the importance of maintaining personal freedom and criminalizing any actions that undermine these freedoms. Moreover, the constitution explicitly guarantees freedom of thought “by all means of expression” in Article 15.

The current Jordanian constitution does not explicitly criminalize violence against women. However, defenders of victims of digital violence can utilize the constitutional principle in Article 6 by arguing that protection from violence necessitates the criminalization of those who commit such acts. This argument can be strengthened by referencing Article 7, which emphasizes the constitutional right to freedom and protection, and Article 15, which guarantees the freedom of expression without borders. Furthermore, the Jordanian constitution guarantees a package of rights that are superior to any other laws, and therefore, the legislator can use this to protect women in the digital space. It is important to note that violence against women is both a cause and result of gender-based discrimination; therefore, constitutional stipulation is crucial to enacting legislation.

International and Regional Treaties and Agreements

Jordan has ratified several international treaties and agreements and has pledged its support for several Security Council and United Nations resolutions that aim to safeguard rights and uphold various principles that can be applied directly and indirectly in legal adaptation and integrating the protection of Jordanian women from digital violence.

The Universal Declaration of Human Rights and its Covenants

The Universal Declaration of Human Rights, promulgated in 1948, serves as the primary international benchmark for numerous treaties and accords related to human rights. Among the nations that have endorsed this declaration is Jordan, which considers Article 19 of the declaration as a cornerstone for safeguarding freedom of thought and expression "through any means and without regard to frontiers."

Although the Declaration itself is not legally binding on the states that ratified it, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights, which emanate from the Universal Declaration of Human Rights and which Jordan ratified in 1975, are binding. The three documents collectively are known as the international legitimacy of human rights and can be relied upon in legal proceedings before Jordanian courts.

Accordingly, it is possible to refer to many provisions of the two covenants, such as Article 17 of the International Covenant on Civil and Political Rights, which criminalizes interference with any person's privacy, including in his correspondence - a principle that can be used to punish the piracy of online social media accounts and digital impersonation. Additionally, Article 19 and Article 20 of the same covenant guarantee the right to freedom of belief "without harassment" and the right to seek and convey information "without regard to borders or means," while also stressing respect for the reputation of others and prohibiting any calls for "discrimination, hostility, or violence."

Article 26 of the present covenant upholds the principle of equality and mandates that signatory nations revise their legislation and guarantee comprehensive protection from discrimination for all individuals, without any distinction based on sex.

Convention on the Elimination of All Forms of Discrimination Against Women

In 1992, Jordan ratified the Convention on the Elimination of All Forms of Discrimination Against Women, commonly referred to as CEDAW. This ratification compelled Jordanian legislative and judicial bodies to take into account women's rights when formulating and interpreting legal provisions. This convention serves as a valuable reference for advocating online freedoms and prosecuting cybercrimes targeting women, by incorporating its various articles into legal arguments. CEDAW's Articles 2 and 3 require ratifying countries to implement a national policy aimed at eradicating gender discrimination and enshrining this approach in their national constitutions and relevant legislation.

Article 5 of this convention mandates that State Parties undertake appropriate measures to foster societal awareness and modify behaviors that contribute to discrimination. Consequently, legislators can promote the establishment of mechanisms to safeguard women online, advocate for the enforcement of laws, implement deterrence and prevention strategies, and launch media campaigns to raise stakeholder awareness. These initiatives aim to criminalize digital violence against women, recognizing it as a form of gender-based discrimination.

Article 6 of the Convention can be employed to classify sexual cyber extortion as a form of trafficking in women and exploiting them sexually, thereby allowing for criminalization. This approach can be complemented by the provisions of the United Nations Convention against Transnational Organized Crime and its accompanying protocols.

United Nations Convention Against Transnational Organized Crime and its Annexed Protocols

This convention, which Jordan acceded to in May 2009, contains several robust provisions that can be employed to penalize sexual extortion and breaches of privacy, particularly those affecting women. These provisions can also be utilized in cases that surpass the jurisdictional boundaries of individual countries, given that the Internet transcends geographical limitations and cyberspace is boundless.

Jordan ratified a protocol in June 2009 with the aim of preventing and punishing trafficking in persons, particularly women and children. This protocol contains two articles that focus on the prevention and combat of trafficking in women and children as well as encouraging cooperation between countries to eliminate transnational organized networks operating in this field. Additionally, Article 9 specifies the provision of protection for women and children to prevent them from becoming victims. These articles can be utilized not only to deter online attackers, but also to provide psychological, technical, and economic support for victims, primarily women, and protect them from further exposure to digital violence.

International Convention on the Elimination of All Forms of Racial Discrimination

Jordan acceded to this convention in May 1974, which obligates signatory nations to take measures to safeguard individuals from any form of discrimination, including discrimination based on sex. This convention can be used both individually and in conjunction with the CEDAW Convention.

Arab Convention for Combating Information Technology Offences

In 2010, the Convention was issued with Jordan signing and ratifying it in 2013. The primary objective of this convention is to combat information technology offences that threaten the security of member states and their interests. While the primary objective of the convention is to protect states, not individuals, there are provisions within the convention that can be adapted to protect women as Internet users from cybercrime. It is important to note that the consequences of these crimes are exacerbated and compounded by the fact that victims are women. The Convention emphasizes the preservation of the safety of societies and their individuals and aligns with Arab and international treaties and covenants related to human rights. This convention shares similarities with the United Nations Convention against Transnational Organized Crime, which applies to crimes committed in more than one country and can be used to protect politically active women who are targeted through organized networks abroad or in multiple countries.

Article 6 of the Convention makes it illegal to gain unauthorized access to private accounts through the Internet and increases punishment if data is tampered with, altered, or distorted, resulting in harm to users or beneficiaries. Article 10 addressed the crime of forgery. These two articles can be cited when prosecuting cases involving digital violence against women, such as deep fake, image composition, and false-statement creation. These acts of violence can lead to severe harm, including murder, in societies in which women are treated unfairly and conservatively.

Article 11 addresses fraud, which may be used to create legal mechanisms to criminalize acts such as phishing, manipulation, and other forms of digital violence perpetrated against women.

Articles 12 and 13, which address the crime of pornography and related offenses, may be particularly relevant to instances of gender-based digital violence, particularly when it involves minors.

Article 14, which criminalizes attacks on the privacy of individuals through information technology, may be used in cases involving piracy, account breaches, and even harassment that occurs through messaging platforms, such as Messenger and WhatsApp.

The Convention provides ample support for victims and their representatives to access digital evidence related to crimes of violence by enabling relevant authorities to quickly and securely obtain, control, and preserve information related to these crimes.

United Nations Treaty for Cyber Crimes

Jordan has played a pivotal role in drafting the treaty since December 2019. In 2022, Jordan advocated the inclusion of language-criminalizing hate speech in the treaty. In January 2024, the final draft of the treaty was presented to the member states for ratification.

Council of Europe Convention on Cybercrime: Budapest (2001)

The Council of Europe acknowledged the international nature of computer crimes in 1976. In 1996, the European Committee on Crime Problems (CDPC) established a committee of experts to address cybercrime. The committee worked from 1997 to 2000 on a draft convention that was subsequently adopted by the European Parliament during the second part of its general session in April 2001. By 2010, 30 countries had ratified the Convention.

The Cybercrime Convention was the first international treaty that aimed to harmonize national laws and those of other countries to address crimes related to computers and the Internet.

The Jordanian legislature and judiciary face several challenges when attempting to apply digital or electronic crime-related treaties and legislation, such as the lack of a clearly defined definition of such digital crimes, the difficulty in collecting evidence in these types of cases, and the absence of international cooperation in investigating such digital crimes.

Most importantly, Jordan has not ratified several international agreements, in addition to the Convention on the Rights of Persons with Disabilities, including the Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (2011) and the Council of Europe Convention on Cybercrime, also known as the Budapest Convention (2010). Although Jordan has indicated its intention to join these conventions and incorporate their principles and protocols into its legislative processes, it has not yet ratified them, making them nonbinding. It should be noted that Jordan is "in the final stages of reviewing the agreements, with the intention of fully signing on to them in the future."[30]

[30] According to a source from the Jordanian Ministry of Foreign Affairs for this research.

Jordanian Legal Framework for Cybercrimes Against Women

In recent times, governments have encountered various approaches to Internet legislation. Most countries regulate the Internet based on their political, legal, ethical, and cultural values. However, the rapid growth of information and communication technology transcends the boundaries of individual nations, thus presenting a significant challenge for governments in their efforts to enact and implement effective legislation to combat Internet crime. This issue arises because countries are unable to keep pace with rapid technological advancements.

Cybercrimes present a significant hurdle for legal systems in both developing and developed nations as the process of legislation takes a considerable amount of time, which impedes the effective prosecution of information-related offenses. In light of this, the responsibility of civil society organizations to raise awareness, organize seminars and workshops, and urge legislative bodies to address digital violence against women cannot be overstated. These organizations play a crucial role in advocating for the amendment of laws and actively participating in their enforcement.

The Jordanian legal system includes a set of laws and national strategies that can be adapted to protect women in the digital space from gender-based violence. However, as of the date of writing this research, there is no explicit legal text that directly criminalizes digital violence against women. Nonetheless, there are various texts in law that criminalize violence against individuals in general, violence against women in particular, or cybercrimes. Therefore, based on the constitutional principles that establish the principle of equality between the sexes and preserve one's freedom and protection, in addition to the international system that Jordan has ratified as previously explained, these various texts can be exploited to form an integrated legal argument that the legislator can use to punish aggressors, protect women, and even compensate them for the digital violence that has befallen them in Jordan.

The development of special legislation to address violence against women has numerous objectives. Most importantly, it will directly address and target all forms of digital violence and not fragment them into scattered legal texts.[31] This is crucial because violence against women is multifaceted, and combating it extends beyond merely criminal methods. A comprehensive approach is necessary because the preventive dimension is a fundamental aspect.

A draft is proposed below for the relevant provisions of the National Women's Strategy, which comprises the most recent Cybercrime Law, No. (17) of 2023, Penal Code, No. (16) of 1960 with amendments, Jordanian Civil Law, No. (43) of 1976, the Protection from Domestic Violence Law, No. (15) of 2017, the Anti-Trafficking Law, No. (9) of 2009, Personal Status Law, No. (15) in 2019, and Communications Law, No. (13) of 1995.

The following laws were selected because they have either direct or indirect relevance to digital violence against women. Although some of these laws do not have specific provisions for this type of crime, they can be adapted and applied to the rulings of such cases. The primary reliance is placed on Cybercrime Law, No. (17) of 2023 as it serves as the main reference for such crimes. If a crime is committed using electronic means outside the context of electronic crimes, Article (26) of this law refers to the judgment of the relevant laws.

[31] Khaled Al-Qudah- digital media expert, member of the Jordanian Journalists Syndicate.

The current state of affairs is plagued by an abundance of legislation and a dearth of clear vision. The question remains unanswered: Is it imperative that a woman be accorded respect for her personal space and her right to self-expression, or is it more pressing that she is shielded from harm? Regrettably, the legislator has yet to arrive at a decision regarding this matter.[32]

The Jordanian Legal Framework for Cybercrimes

Organizing electronic information, records, and correspondence and conducting banking operations electronically require security to guarantee that unauthorized individuals do not access this information. There must also be legal protection against the hacking of these systems and electronic records, as well as against intercepting electronic correspondence for the purpose of viewing, copying, or destroying information. The Cybercrime Law criminalizes various forms of offense in electronic commerce. Legal protection extends to personal information and private uses conducted over the Internet, in addition to electronic records and systems related to commercial and economic activities and trade secrets. It is essential to have strict legal measures to protect against these types of cybercrimes.

To ensure proper protection of the content mentioned above and complement the legislative environment related to controlling cyberspace activities in Jordan, the Hashemite Kingdom of Jordan issued three laws regulating digital space: the Temporary Information Systems Crimes Law of 2010,[33] the permanent law of 2015, and the amended version of 2023.

The provisions of the temporary law enacted in 2010 were incorporated into the amended versions of the law, including 2023. These provisions include criminalizing unauthorized entry to a website or information system and deleting, modifying, or copying data (Article 3), publishing data or information containing defamation, slander, or contempt (Article 8), or pornographic content (Articles 9 and 10), among others.

Cybercrime Law, No. (27) of 2015 was enacted in Jordan on June 1, 2015, as a permanent law based on the Temporary Information Systems Crimes Law of 2010. The law was implemented to strengthen the legal framework for addressing cybercrime and replace the 2010 law under Article 94 of the Constitution. The amendments made to the Temporary Information Systems Crimes Law outlined the penalties for assault on electronic records, systems, and websites, based on their function or content. For instance, penalties were imposed for assaults on electronic records or systems that affect bank transfers or electronic clearing or for assaults on information that affects national security or foreign relations, even if it is not available to the public.

[32] Attorney Lynn Al-Khayyat.

[33] To access the full text of the law, please refer to this article.

The 2015 legislation not only prosecutes the breach of the information network (the Internet) and electronic records as the location of the offense but also imposes penalties for the perpetration of other crimes detailed in the law when executed through information technology. These offenses include the distribution of defamatory, slanderous, or scurrilous materials as well as the promotion of prostitution via the Internet.

Subsequently, Cybercrime Law, No. (17) was enacted in 2023 to clarify the location of the crime, its methods, and the investigation procedures involved. The legislator aimed to keep pace with technological advancements by detailing the types of crimes and penalties in various stages of law development, culminating in the most recent version issued in August 2023. The increase in penalties under the current law compared with previous versions is attributed to economic inflation over the past decade, from 2010 to the present. However, this increase also serves as a deterrent and preventive measure against various forms of violence affecting both women and men on social media and the internet in general. For instance, the penalty for defamation, slander, and contempt has increased from a fine of 100 dinars in 2010 to 5000 dinars in 2023.[34] This finding is supported by expert testimonies gathered by research specialists, who noted that increasing penalties, even if not specifically targeting women, will automatically afford them greater protection from electronic crimes given their status as an easily targeted group.[35]

Although no cybercrime legislation specifically addresses the protection of women in the digital space, the most recent law enacted in 2023 serves as a basis for recommending pertinent provisions to lawmakers and legal authorities. These provisions can be tailored to criminalize digital violence that targets women. These provisions can be used individually or in combination with the previously mentioned constitutional principles, especially those of gender equality and the protection of women. In addition to Jordan's commitment to international charters and treaties, it ratified some of the other relevant laws discussed later, such as the Penal Code and Communications Law.

As noted by the experts in this study, the current Cybercrime Law underscores the necessity of revising the current legislation to specify provisions that provide comprehensive protection for women from digital violence in the areas of prevention, punishment, and compensation. This can be accomplished by incorporating deterrent measures for those who commit or facilitate the commission of violence or incitement to it, criminalizing violence in its various forms with increased penalties, and providing compensation to the victims and offering support to help them recover from psychological, social, and other damages that are particularly severe in Jordanian society.

Cybercrime Law 2023

Until the issuance of laws addressing digital violence against women or amendments to the current laws, the 2023 law includes provisions that protect women from digital violence and criminalize this behavior, with the aim of punishing its perpetrators. These provisions can be found in articles that cover the act of intentionally capturing, intercepting, or eavesdropping on information sent via the internet or any other information system (Article No. 6). Article 7 of the same law also criminalizes access, hacking, or intercepting the flow of data with the intention of disclosing information that individuals do

[34] To compare the texts of the two laws: 2010 | 2023

[35] Noha Mahrez (Director of the Women's Solidarity Institute) and Khaled Al-Qudah (digital media expert and member of the Jordanian Journalists Syndicate).

not wish to disclose. This can include doxing, which involves publishing personal information with the intention of causing harm.

The law prohibits knowingly disseminating or publishing through an information system or the Internet any audio, visual, or written material that depicts pornographic acts or sexual exploitation in general (Article 13), particularly when the individuals involved are under the age of 18 (Article 14).[36]

Article 13 of the criminal code states that a victim of prostitution who is over the age of 18 can pardon the perpetrator, which eliminates the public's right to pursue justice in the case. This provision is concerning, as it does not take into account the long-term harm caused to the victim and their family and may incentivize perpetrators to pressure victims into dropping the case.

The legal provisions of the new Cybercrime Law address a variety of sensitive issues, including blackmail, particularly when it involves children and juveniles. However, the law does not include provisions to increase penalties when the victim is a woman. It is interconnected with the overall system of legislation, practices, and public policies.[37]

To a significant degree, Article 15 of this law can be adopted by the judge in cases involving digital violence against women, such as the publication of false news or defamation, slander, or contempt. These types of incidents, which often target women holding prominent positions in politics, journalism, and the public sphere, can be subject to legal action.

The dissemination of private information with the intention of defamation, insult, or personal gain is prohibited by the law (Article 19). This type of offense is considered compound, as it encompasses illegal activities, such as hacking, eavesdropping, or unlawfully obtaining personal information, which are criminalized under Articles 6 and 7 of the law, as well as the publication or promotion of such information with malicious intent or for personal benefit, which is criminalized under Articles 13, 14, & 19.

Article 20 of the legislation addresses the issue of financial extortion or coercion through the threat of publishing or republishing illegal content or false news. Specifically, this article delineates the jurisdictional scope of such crimes, whether they occur within or outside the Hashemite Kingdom of Jordan. Consequently, this article can be applied in conjunction with international and Arab agreements pertaining to cybercrime that Jordan has ratified. Moreover, Article 38 explicitly covers cybercrimes committed "outside the kingdom and caused damage to any of its interests or its citizens or residents or the effects of the crime occurred in it wholly or partially."

The provisions outlined in Article 33 of this law enable the public prosecutor or the competent court to address the perpetrators of the crime, regardless of their location, either within or outside the Kingdom. Additionally, these provisions allow the issuance of orders to those responsible for the platforms or channels used to commit the crime, deliver evidence, preserve data, delete harmful content, and maintain confidentiality. If necessary, the public prosecutor or court may issue an order to ban the information system, website, communication platform, or services from the national network. This

[36] For example, in October 2022, the Cybercrime Unit monitored pictures of a juvenile performing pornographic acts that were spread across social media sites. They tracked down the event in cooperation with Criminal Security and the police, and the matter was dealt with. While those who photographed and published the pictures were not punished, the pictures were used to track the event on the ground, which confirms the connection between the digital space and the real world.

[37] Journalist Hadeel Ghabboun.

measure is intended to ensure compliance with the law in Article 37, which requires social media platforms with more than 100,000 subscribers from Jordan to establish regional offices for easy coordination.

Article 17, which pertains to hate speech, does not explicitly address gender-based violence on the Internet. However, it does criminalize "incitement to violence," providing a means to hold individuals accountable for inciting violence on social media platforms against feminists or women's rights advocates. Extremists and power centers often target these individuals, seeing their activities as a threat to the status quo and social power dynamics. In addition, Article 27 imposes penalties on anyone who intentionally aids, interferes with, or incites the commission of crimes outlined in the law. This means that the enforcement and implementation of the law can serve as a deterrent and protect not only the perpetrator of the crime, but also the broader environment in which it occurs. It is crucial to be aware of these two articles (17 and 27), as highlighted in the study's introduction, to confront the type of crime that society often tolerates and does not consider a real crime because of its occurrence in virtual spaces.[38]

Legal professionals contend with the challenge of defining digital violence against women legislatively. This difficulty arises from the conflation of this crime with other legal concepts such as physical gender-based violence and financial fraud. The psychological and social repercussions of digital violence are profound, as evidenced by the psychological crises that victims experience.[39] Thus, it is essential to establish a precise definition of digital violence and classify its various forms within the boundaries of law.

> *Undoubtedly, it is crucial to develop and amend relevant legislation on domestic violence. Although the recent amendment to cybercrime law is certainly beneficial, it is insufficient on its own. To combat this issue effectively, amendments to the penal code are necessary.*[40]

The current law doubles the penalty for any individual who commits a crime while exploiting their job, work, or the powers granted to them if the victims are numerous or if the same offense is repeated (Article 28). This can be particularly relevant in instances of digital violence against women, which are perpetrated by executives or those who hold authority over them, whether in the workplace or in various community institutions, such as educational, religious, and public social institutions, or even in the private sector and economic institutions. As a result, it is easy to connect the disparity in social power based on gender, particularly in patriarchal societies like Jordan, with the victimization of women in public spaces, including digital spaces, as they are socially weaker and more susceptible to digital violence.

The Cybercrime Law comprises Article 26, which addresses the offenses detailed in other legal frameworks committed within the digital realm and through information networks and technology. This article refers to the relevant legal authority. Furthermore, Article 30 mandates the imposition of the harshest penalty when the offense falls under the purview of both the law and another legal framework.

[38] Refer to the appendix for the full text of the articles.

[39] Noha Mahrez- Khaled Al Qudah.

[40] Attorney Muhammad Abu Zannad- Member of the Bar Association Council.

This provision allows for the application of other laws to criminalize digital violence against women, which is discussed in further detail later.

Despite the legal protections afforded by the law, which include a special penal code that branches off from the penal code, the failure to address violence directed against women in a specific and explicit manner creates a number of technical and human rights loopholes. When taken together, these loopholes pose a threat to women by not criminalizing digital violence against them, thereby allowing perpetrators to escape punishment.

As a victim, a woman imposes a special obligation on the legislator to intensify and specialize efforts to address this issue, given the seriousness of the crime and its impact on both the victim and her public image. Violence against women is not limited to the immediate consequences of the crime but extends to long-term psychological effects on the victim and societal stigmatization that can result in murder. Furthermore, the harm caused by violence can extend to the victim's family and even to the entire tribe, given the conservative tribal nature of Jordanian society.

> *There is a real issue concerning the lack of legal deterrents and adequate public awareness to bolster the initiatives undertaken by non-governmental organizations to promote an understanding of digital violence and cyber blackmail.*[41]

The situation is further compounded by the fact that the laws governing digital violence are largely unknown, particularly the Cybercrime Law, which is relatively recent legislation. Unfortunately, the public, particularly women, has limited knowledge of this law. Furthermore, this law does not explicitly address the issue of digital violence against women. Given the rapid pace of technological advancements and the emergence of new electronic devices on a daily basis, it is difficult for the law to encompass all the aspects of digital violence.[42]

Penal Code

The Jordanian Penal Code is a legal framework that addresses a range of offenses and violations that may arise from interactions among individuals. However, many of its provisions were developed prior to the emergence of the Internet and the rise of gender-based digital violence. Therefore, the majority of these articles are general in nature and do not consider the use of digital means.

The Jordanian Penal Code criminalizes various forms of violence in which women, who are more vulnerable than men, may fall victims. The latter category addresses all forms of violence against women in Jordan. Although the Penal Code does not have any explicit laws pertaining to digital violence against women, Articles 73 and 77 discuss the scope of committing the crime, encompassing automated media such as audio, written materials, images, or videos.[43]

[41] Attorney Nidaa Al-Shuwaikh.

[42] Noha Mahrez- Director of the Jordanian Women's Solidarity Institute.

[43] Refer to the appendix for the full text of the articles.

Although there are no specific laws regarding digital violence against women, Articles 188, 189, and 190 on defamation, slander, and contempt can be used in cases of digital violence against women. These articles not only provide clarity on the crime and its proof but also give the judge broad discretion to classify any form of publication in the public domain or direct contempt in private.

Furthermore, Article 73 clarifies the nature of public communication, including that on the internet and social media. According to the specified article, any actions or words that can be transmitted through mechanical means and observed by others are considered forms of publicity, including dissemination of information through digital means.

Article 82 of the law may impede the pursuit of justice for women subjected to digital violence and incitement by influencers, even if the violence itself is perpetrated by others. This is because the law does not hold individuals accountable for inciting or facilitating the commission of a crime, even if it falls within the least severe category of offenses. Article 81 of the law, which precedes Article 82, outlines the principle of shared criminal responsibility in misdemeanors and felonies and the preference for the application of special laws, such as those related to cybercrimes, over general provisions.

Article 82 of the law is viewed by influencers as a hindrance to attaining justice for abused women in the digital realm. This article does not penalize those who incite and facilitate the commission of a crime. It is intended only for least severe offenses. Article 81 stipulates that criminal liability applies to both misdemeanors and felonies, and the presence of its counterpart in a special law (cybercrimes) indicates that it takes precedence in such cases.

Article 306 addresses acts that are contrary to modesty and criminalizes harassment of a sexual nature that involves sending inappropriate images or videos even words, whether by “declarative reference or insinuation by any means.”

Article 311 imposes penalties for sexual blackmail, which involves the use of threats or intimidation to force someone to engage in sexual acts. Article 319 criminalizes the sale, possession, and distribution of materials or images that are indecent or obscene, including the creation or dissemination of false images of women for defamation or blackmail. Finally, Article 415 explicitly criminalizes any threat that adversely affects the reputation or honor of an individual or their relatives.

Unauthorized access to private spaces and information through eavesdropping, audio recording, or photography is considered a criminal offense under Article 348 bis. This article is particularly significant because it often serves as the starting point for various digital fraud and deceit operations, such as hacking devices to obtain banking or personal data that can be exploited for blackmail or theft of funds. Regrettably, many women are vulnerable to phishing scams because of the lack of digital literacy and their susceptibility to emails or messages that exploit their fear of their personal information being leaked, such as message warnings of a hacked device and instructions to click on a link to prevent it. This fear, coupled with societal norms that prioritize women's privacy, often leads to a hasty response and an increased likelihood of falling victim to scams. Therefore, this type of digital crime has gender-related dimensions rooted in cultural and traditional customs, as well as a lack of awareness.

Article 348 bis of the criminal code punishes intrusions into private spaces that involve acts such as peeping, audio recording, or photography. This article is of significant importance since it addresses the initial stages of digital fraud and scam operations, which often involve hacking devices to access banking or personal information that can be exploited for blackmail or financial gain. Unfortunately, many women fall victim to this type of cybercrime because of a lack of digital culture and the manipulation of trolls. Women often interact with emails or messages that claim that their device has been hacked,

and clicking on a specific link can prevent further hacking or the release of personal photos and videos. However, such links often result in device hacking or extortion. The cultural emphasis on women's privacy and the fear of personal photo and video leaks contribute to the vulnerability of women to this type of cybercrime. Therefore, it can be argued that this type of cybercrime has gender dimensions, both due to cultural and traditional factors, and the lack of awareness about such crimes.[44]

Although the content of many materials is comprehensive and extends to digital violence, it fails to capture the specificity of gender-based digital violence. Consequently, perpetrators are penalized in a manner disproportionate to the significant negative impact that this crime may have on women in particular. Moreover, the materials do not address the need for compensation and protection of victims from the psychological and societal harm resulting from these crimes. Considering social reality, it is essential to impose severe penalties for crimes committed against women, as they are a group that may be subjected to greater social consequences than those experienced by males who are subjected to the same type of violence.

Communications Law, No. (13) of 1995

The Communication Law of 1995 in Jordan provides constitutional protection for the right to privacy of communications, including the protection of women as members of society from attempts to hack and eavesdrop. Articles 56, 75, and 76 specifically address the need to protect the secrecy of communication and prohibit threats, insults, and messages that violate morality or cause panic. Additionally, the law criminalizes the deletion and alteration of content, and even encourages such information.[45]

The current legal provisions do not provide adequate protection for women, and penalties for cybercrimes such as threats, sexual blackmail through communication, altering content, and hacking of accounts are not commensurate with the severity of the offense and its consequences. Furthermore, despite the need for more stringent penalties for repeat offenders, there is no provision for compensation of victims of such crimes.

Electronic Transactions Law, No. (15) of 2015

Statutes are commonly referred to as the Electronic Transactions Law, the E-commerce Law, or the Electronic Contracts Law pertains to electronic transactions, such as electronic signatures and electronic authentication.[46] However, this law does not apply to personal transactions or social communication through which women are frequently targeted by digital violence. Nonetheless, Article 24 of the law, which penalizes individuals who engage in fraudulent activities, is often used in digital phishing operations that affect both men and women. Research[47] indicates that women are more susceptible to phishing and digital fraud than men, as they are typically less involved in financial transactions in society. Furthermore, they are also more likely to fall victim to emotional phishing or blackmail, through which the troll uses financial needs to ask the victim woman to help him in exchange

[44] In January 2022, the Cybercrime Unit warned of the spread of messages and emails that troll recipients of posts under the pretext that their devices have been hacked and request sums of money in exchange for not publishing the contents of the device that was allegedly hacked.

[45] Refer to the appendix for the full text of the articles.

[46] You can access the full text of the law.

[47] See: Al-Ghad newspaper: "Salamat launches a campaign highlighting digital violence against women," February 2022. And The Kingdom: "Digital violence: Another challenge facing women in Jordan and calls for harsher penalties," May 2023.

for continuing the relationship with her, presenting false documents. In reality, digital fraud is often spread through social media posts, especially Facebook, text messages, and WhatsApp circulations that contain false content and electronic links, and are designed to psychologically manipulate recipients, such as news about lost children or providing aid to the poor. Women, particularly those with limited digital experience, are more likely to interact with such content.[48]

Civil Law, No. (43) of 1976

This law governs financial dealings between individuals in Jordanian society and regulates their conduct. Article 3 of the law serves as the foundation for other laws and is capable of governing all rules applicable to all individuals, regardless of their professional, social, or economic status. In the absence of any specific provisions in other laws, such as the Commerce Law or Labor Law, civil law is consulted to find the relevant ruling regarding a particular matter pertaining to its subject matter.

Although limited to financial matters, the law includes several provisions that address the harm and financial compensation arising from digital violence against women.[49] Specifically, Article 267 deals with ensuring moral harm and imposes liability on anyone who "violates others' freedom, appearance, honor, reputation, social status, or financial standing." This is because electronic platforms and social media accounts can be considered personal property under Article 54 of the law, which covers both tangible and intangible assets that can be owned legally. Consequently, any unauthorized access to or defamation of reputation that leads to a reduction in financial returns from digital content, such as advertisements or followers, can be addressed through this law. Additionally, articles on coercion, specifically 279 and 280, can be referenced in the context of criminalizing identity theft and unauthorized access and use of digital accounts and websites; the severity of the penalty increases based on the level of harm caused, such as when the victim holds a prominent position, has significant social influence, or belongs to a conservative society.[50]

The Domestic Violence Protection Law, No. (15) of 2017

Digital violence is often associated with various forms of domestic violence. This phenomenon is characterized by the tendency to blame the victim and punish her by her family after the occurrence of digital violence or physical assault cases that resulted from incitement on digital platforms. Additionally, there are instances of digital violence that occur due to violence in reality, such as hacking and digital blackmail, which are preceded by threats or harassment. Given these circumstances, it is essential to highlight the importance of legal protection against domestic violence in this context.

The issue of applying the articles of this law to instances of digital violence is complicated by the fact that such violence typically occurs in the public realm of the Internet, whereas the scope of family law, which primarily operates in the private sphere, is limited. Article 2 of the law defines domestic violence as “crimes committed by a family member against any of its members.” Thus, the practicality of using this law may be limited to instances of violence between spouses during disputes or divorce proceedings, or cases in which family members, particularly males, perpetrate violence against women who have fled their families for any reason. This type of violence is often carried out through online and digital

[48] The Cybercrime Unit warns of many of these fraudulent posts, for example news about the distribution of financial aid.

[49] Such as Article 62 and Chapter Three under the title “Harmful Act,” especially Articles 256, 257, 265, 267.

[50] Refer to the appendix for the full text of the articles.

communication platforms such as WhatsApp and text messages. Numerous cases have emerged in which women have been subjected to digital violence before being physically harmed by family members.

The provisions of this law provide for a quicker and simpler filing of complaints through the Family Protection Department while also protecting the confidentiality of family matters. Furthermore, it offers special protection for women, such as shelter and pledges of non-harm as well as legal assistance.[51] It is important to note that the responsibility to report violence includes health, education, and social service providers in both public and private sectors. Additionally, they are required to provide psychological and social support to victims and utilize modern technology to gather testimonies from minors or those who may feel intimidated.

This legislation serves as a critical first step in advocating for issues faced by female victims of digital violence in Jordan. By increasing awareness among lawmakers and those responsible for receiving complaints and reports from police and other agencies, the law seeks to ensure that instances of gender-based digital violence are taken as seriously as physical cases. As such, it is recommended that certain provisions of this law be revised to explicitly address digital violence and further protect women, who are often the most vulnerable members of their families. Through education and awareness, those responsible for providing protection are better equipped to address this issue.

The Personal Status Law, No. (15) of 2019

This law is most indirectly associated with digital violence against women, as this violence is gender-based and built on society's perception of the stereotypical social roles of males and females in society and the balance of power between them. Like the Domestic Violence Protection Law, its scope of application falls within the private domain, such as marriage, divorce, and inheritance, and it regulates the relationship between individuals and their families.[52] Article 126 of the law, which addresses separation due to discord and disputes, may be relevant to cases of digital violence. When determining the appropriateness of separation, the court considers the severity of harm and offense, which is influenced by cultural norms. Harm here, especially moral harm, is defined by the law as any "disgraceful behavior or conduct that is contrary to good morals and causes moral harm to the other party." It is important to note that this research does not advocate for hasty separation or family dissolution but rather emphasizes the need for serious consideration of digital violence and its impact on women in marital relationships, particularly those involving verbal or written abuse rather than physical harm. Legislators should also consider the digital evidence of violence in family cases.

The Personal Data Protection Law-Draft

The draft outlines regulations pertaining to the processing and retention of personal data. The House of Senate and Representatives approved the draft law, which, at the time of writing this research, was awaiting publication in the Official Gazette and discussion. It is crucial to mention that the provisions of the law do not extend to individuals who process personal data for non-personal reasons, potentially limiting its scope to safeguarding against digital gender-based violence.[53]

[51] The text of the law can be viewed via this link.

[52] To view the full text of the law, please refer to this link.

[53] Jordanian Open Source Society.

The National Strategy for Women 2020-2025

Before delving into the legal framework for digital violence against women and girls in Jordan, it is essential to examine the National Strategy for Women. Although the National Strategy for Women is not a law, as a government policy and commitment approved by the Council of Ministers, it is considered a crucial reference framework for enhancing the circumstances of Jordanian women at various levels. It has been produced in collaboration with several relevant institutions, including the National Assembly, both the Senate and the House of Representatives. Accordingly, any laws that have been passed must consider this strategy and its guiding framework. The primary objective of the National Strategy for Women is to create "a society that is free of discrimination and gender-based violence, where women are afforded full human rights and equal opportunities to achieve comprehensive and sustainable development."

The Jordanian National Commission for Women's Affairs, while formulating its strategy under the direction of the Prime Minister and the supervision of the Ministerial Committee for the Empowerment of Women, aimed to align their strategy with the Jordanian Constitution, national plans, and international obligations. This strategy serves as a roadmap for the Jordanian government to achieve gender equality and to empower women. Efforts are being made to accomplish this goal through collaboration between executive and legislative authorities and partnerships with national institutions, civil society organizations, and the private sector.[54]

The strategy aims to achieve the following objectives:

1. Ensure that women have access to their human, economic, and political rights, thus enabling them to participate and lead freely in a society free from gender-based discrimination.
2. Eradicate all forms of gender-based discrimination and ensure that women live a life free of such discrimination.
3. Promote customs, attitudes, and positive social roles that support gender equality and women's empowerment.
4. Establish and maintain institutions that implement and ensure the sustainability of policies, structures, and services that promote justice and gender equality and empower women in a manner that aligns with national and international commitments.

To assess the progress towards these objectives, the strategy identified a series of outputs, one of which was output 2.1, which specifically requires the development of "efficient means for preventing, protecting against, and responding to gender-based violence in the private, public, and digital realm." This was to be achieved through several inputs, such as "enhancing the understanding of relationships based on respect and rejecting gender-based violence within societies and addressing its various aspects in the public and digital realm."

The fourth objective underscores the duties of various institutions and highlights the importance of establishing mechanisms for evaluating and monitoring Jordan's dedication to fulfilling its national and international obligations for women.

[54] National Strategy for Women in Jordan 2020-2025

Social Media Policies and Instant Messaging Applications

Social media platforms offer fertile grounds for gender-based digital violence. Many individuals are unaware of the underlying mechanisms of these platforms and lack a digital security culture or Internet safety principles. The prevalence of digital violence on these platforms increases with their increasing usage, which spans across different age groups. Despite the constant pressure on companies owning these platforms to enhance user safety and minimize their potential negative impacts, the efforts made thus far have fallen short on several fronts, including the issue of gender-based digital violence.

While Facebook's community standards are designed to protect all users by enforcing general policies, it is worth noting that certain standards are tailored to children without providing additional protection for women on its platform. Similarly, Twitter's rules fail to provide special protection for women, but its hate behavior policy acknowledges the privacy and reality of women, prohibiting posts that promote and encourage gender-based digital violence.[55] Despite ongoing efforts to address digital violence against women in Jordan and globally, such violence persists on various communication platforms, including Facebook and Twitter. Currently, there are no guarantees or practical measures to address this issue effectively.

Instant messaging applications such as WhatsApp, which is owned by Facebook, pose a unique threat to women. These applications share many features with social media, yet they may differ in certain aspects. For instance, WhatsApp is particularly prevalent in Jordanian society, with 78% of social media users in Jordan utilizing this application. With such widespread use, WhatsApp is a highly influential digital medium in Jordanian society.[56]

WhatsApp employs end-to-end encryption technology[57] that ensures that only two communicating parties can access their correspondence. Advanced algorithms are used to secure messages, thereby allowing millions of users to communicate without surveillance from any third party. This technology does not permit tracking of any malicious activities on the platform by the company or law enforcement agencies. Unfortunately, this lack of tracking capability has led to an increase in the number of cases of digital violence based on gender. It is difficult to monitor or limit such incidents on encrypted platforms such as WhatsApp.

[55] Hateful conduct policy, Twitter.

[56] Khaled Al-Qudah- digital media expert, member of the Jordanian Journalists Syndicate.

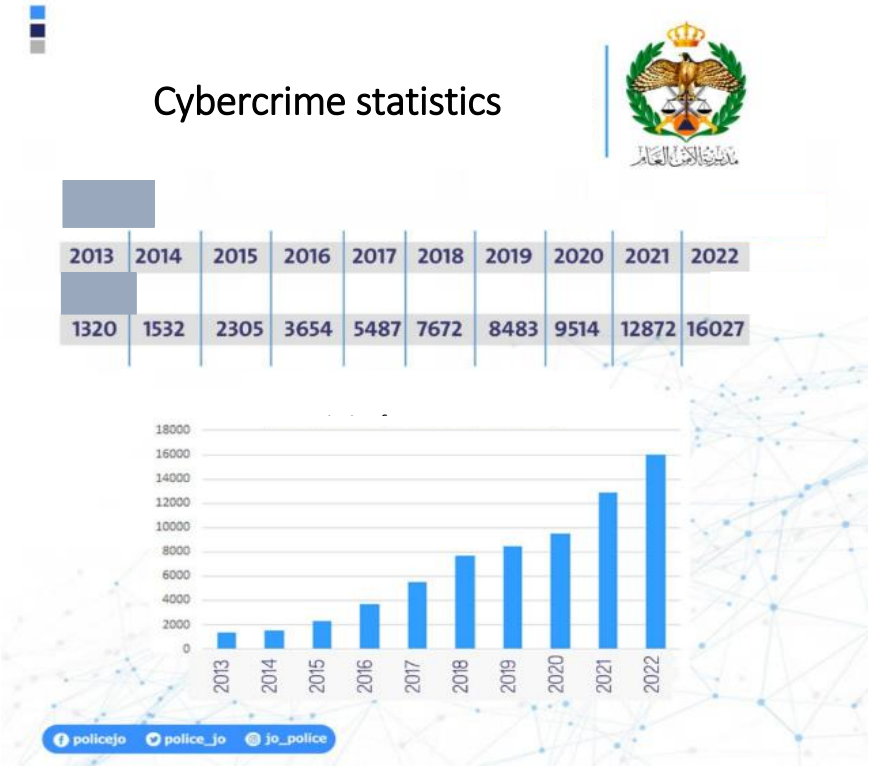
[57] About end-to-end encryption, WhatsApp.

Institutional Framework and Legal Reference for DVAW in Jordan

The lack of information and databases related to gender-based cybercrimes, known as digital violence against women, makes it difficult to develop policies and strategies to deal with, prevent, punish perpetrators, ensure they do not escape punishment, and ensure that targets receive appropriate compensation. Despite this scarcity, statistics from the Cybercrime Unit of the Criminal Investigation Department in Public Security in 2022 show that cybercrime cases have increased over the past seven years by about six times. In 2015, there were 2,305 cases, but by 2022, this number had risen to 16,027. The published reports do not include gender details, which must be addressed to facilitate the diagnosis of problems and constantly renewed phenomena in these digital spaces.

The Cybercrime Unit attributed the increase in reports to the widespread use of technology, digital solutions, smartphone applications, and the expansion of social media platforms. Additionally, educating citizens about their rights and ability to litigate has increased the percentage of crimes recorded at the unit and encouraged victims of this type of crime to file legal complaints.

The unit also pointed out the emergence of new criminal methods, such as digital witchcraft, sexual exploitation via social media platforms, and theft of electronic wallets, noting the increase in electronic fraud cases, which reached 2,118 cases in 2022. The number of electronic blackmail cases increased significantly, reaching 1285 incidents. Additionally, there were 3769 cases of defamation, slander, and contempt, as well as 3466 threat cases, and 2115 hacking incidents. This increase in cases can be attributed, in part, to the growing awareness of the importance of reporting such incidents, which highlights the significance of digital safety awareness.[58]



[58] Public Security Directorate, Cybercrime Unit, "The Public Security Combating Cybercrime Unit publishes its annual statistics for the year 2022," January 2023.

The lack of awareness among all categories of women regarding digital violence, as well as their inability to effectively utilize modern technologies and programs, has exacerbated the problem of this type of crime. This is particularly acute in rural areas, where access to resources and technology is limited. Moreover, the difficulty in dealing with these crimes is exacerbated by the fact that reporting is necessary for resolution.

The limited understanding of legal articles and their insufficient protection against digital violence against women and children, particularly among those who receive reports and those who interact with victims directly in relevant institutions, hinders the achievement of guaranteed freedom and protection for women in the digital realm, as per the constitution. Furthermore, the shortage of qualified and technically competent individuals in the field of information systems within these institutions jeopardizes the right to secure online privacy and safety, as well as the ability to hold perpetrators accountable for cybercrimes such as harassment, sexual harassment, and extortion. This also restricts women's safe access to information and freedom of expression. The lack of safety and preparedness among women to confront digital violence, the erosion of their confidence in the relevant agencies, and their ability to protect them and maintain their confidentiality pose a threat to their physical safety and psychological well-being. This undermines their presence and participation in cyberspace.

Despite the efforts of various bodies, including female police cadres, to enhance their knowledge of personal and information security.[59] Therefore, training workshops are essential. In addition, the presence of females in the regulatory and security sectors is crucial for encouraging victims of cybercrime to report their experiences. Having a female recipient in the report helps to understand the psychological and social implications faced by female victims in Jordanian society as a result of cybercrimes, including digital violence against women.

[59] For example, the Women Police held training for twenty-seven participants from the security sector in February 2023, covering cybercrime.

The Cybercrime Unit

The Cybercrime Unit was established in 2008 as the primary body responsible for combating cybercrime, including digital violence, against women. The Public Security Directorate's Cybercrime Unit defines cybercrime as any act that is likely to harm civil or moral conditions as a result of direct and indirect information technology's intervention.[60]

The unit's literature states that the goal of establishing the Cybercrime Department in the Criminal Investigation Department in 2008 and developing it into the Cybercrime Unit in 2015 was to combat cybercrime and educate the community about its risks. The unit operates through a participatory approach with various local and international institutions, including private, financial and banking, telecommunications companies, and civil society institutions.

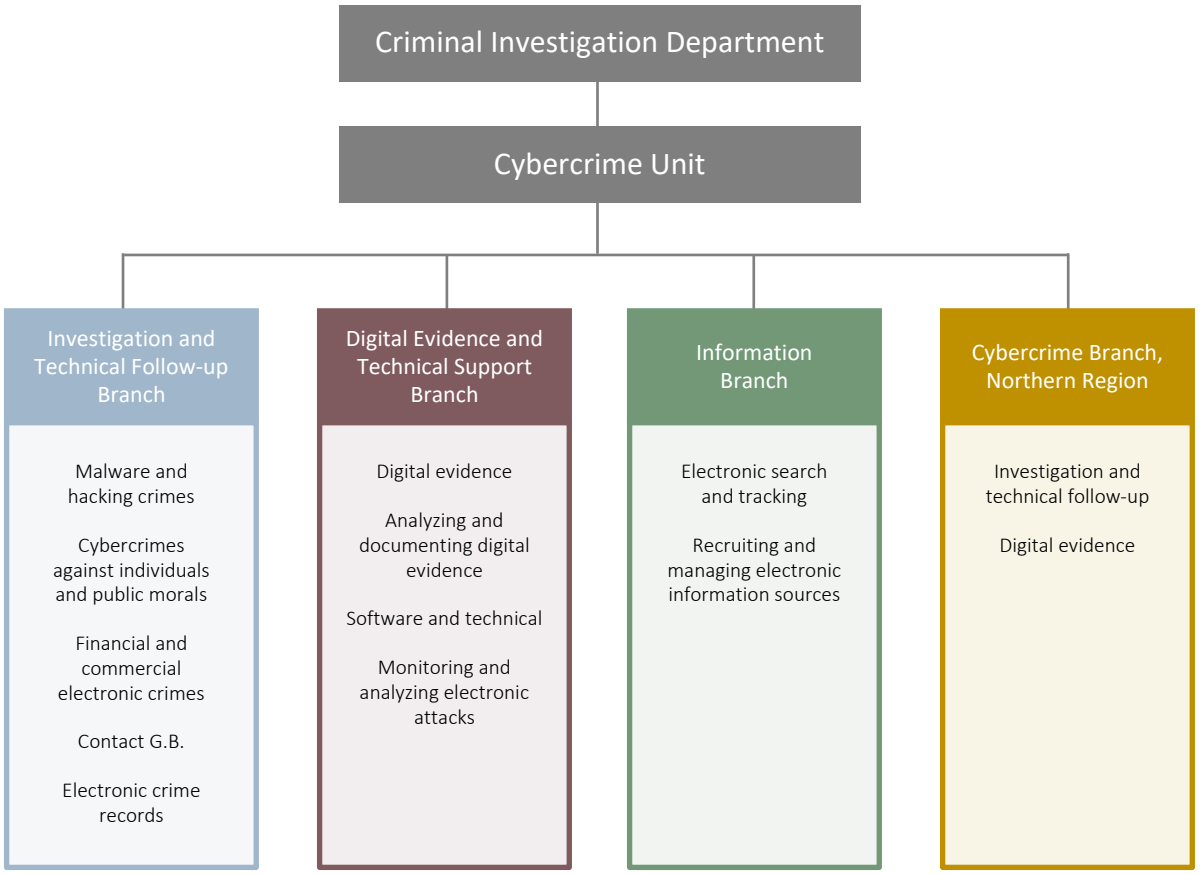
This approach aligns with criminology studies, which define digital violence as "the intentional behavior carried out by an individual or a group through social media platforms and their various tools with the aim of causing physical or moral harm to others." As long as violence is considered a form of criminal activity, the same principles that apply in the physical world also apply in the digital realm. This includes the practice of gender-based digital violence against women, which is an extension and consolidation of violence directed against them in the real world. In accordance with laws (amended for the Public Security Law of 2023) and Law, No. (38) of 1965,[61] the Cybercrime Unit follows the Criminal Investigation Department in the Public Security Directorate and serves as a specialized judicial officer that works in collaboration with public prosecution.

The unit comprises the following four main divisions:

1. **Investigation and Follow-up Branch:** This largest and most active branch responsible for investigating complaints and providing technical reports to public prosecution. It also monitors criminal trends and patterns regardless of their purpose or whether they involve crimes against people, money, public morals, or public order.
2. **Digital Evidence and Technical Support Branch:** This includes experts in cybersecurity and specialists in programming, ethical hacking, and licensed professionals who document digital criminal evidence discovered by the Investigation and Follow-up Branch. This branch is also responsible for following up on organized electronic attacks in coordination with the rest of the unit's organizational structure.
3. **Information Branch:** This branch conducts operations similar to those of the Digital Evidence Branch, except that this branch conducts electronic search and tracking operations, manages information sources, and verifies the quality of sources that affect the recipient in the local digital space.
4. **Cybercrime Combat Branch, Northern Region:** This branch is geographically oriented and serves the northern region. It includes units for technical investigation and follow-up as well as a department for digital evidence.

[60] Cybercrime Unit- Public Security Directorate.

[61] Bureau of Legislation and Opinion- Jordanian Legislation.



It is important to note that the unit in question receives significant attention from the Public Security Directorate as per their policies. However, to improve its work, the unit must expand its circle of human cadres and allocate more financial resources, as reported in general budgets. It is recommended that logistical, human, and material support be increased in this unit. With thousands of cases to handle each year, investigation cadres face immense pressure, and their efforts to spread awareness through seminars and courses with civil society institutions are commendable. Nevertheless, adding this additional responsibility to their already burdensome workload increases their operational burden and strains the limited expert salaries in this unit.

Some investigative methods for technical tracking

- Various techniques for investigative purposes are implemented by the hosting companies of accounts or websites, such as Facebook, Instagram, and Snapchat, for technical tracing.
- This approach relies on electronic phishing and social engineering, which are highly dependent on the individual's expertise and are notably challenging in terms of both effort and time required.
- Investigative methods typically involve the use of digital loggers, sources of electronic messages and digital traces, as well as the collection of information and data in order to determine a user's digital identity.
- The unique digital identifier, comprising a specific date and time, serves as a critical piece of evidence for determining a user's identity. This identifier, known as the Internet Protocol (IP) address, can only be translated into the user's name through the cooperation of the Internet service provider.
- A single digital address cannot be given along with a specific time and date due to technical constraints of the tracking process. Nevertheless, the target digital address where communication was made can be provided up to a certain extent. However, it is not feasible to provide additional addresses beyond that.

In terms of procedure, the Cybercrime Unit handles confidential reports and complaints submitted by Jordanian citizens with the utmost discretion, ensuring that the identity of the complainant remains anonymous. For instance, the unit tracks messages sent to the victim's phone by blackmailers in digital blackmail cases, allowing them to identify and apprehend the blackmailer.[62] Compensation is determined by a civil ruling issued by a magistrate court[63] in a separate case, based on what was decided by the criminal court that examined the crime.

The process of submitting a complaint about cybercrimes in Jordan involves visiting the nearest security center, where the complainant will be transferred to the Cybercrime Unit through an official letter. Alternatively, one may go to the closest public prosecutor's office to their place of residence and file summons with the lawsuit. If an individual encounters such incidents, they may contact the Cybercrime Unit directly at any time through WhatsApp number 0770993331.[64]

[62] Nofal Law Office.

[63] The civil "rights" courts of first instance in Jordan are called "conciliation", conciliation of rights, conciliation of punishment, and it is an amendment to the formations of the courts that came to deepen the need for the courts to reach reconciliation and societal peace based on their decisions.

[64] Cybercrime Unit- Public Security Directorate.

Security issued a number to inquire about electronic crimes

The Criminal Investigation Department's Cybercrime Unit has established a dedicated phone line, 065633404, to provide assistance to citizens and address any inquiries, with a particular focus on cybercrimes.

The implementation of this initiative falls under the Public Security Directorate's policy of enhancing and upgrading security services to fulfill the citizens' aspirations for a superior security system.

According to Major Anas Al-Halahla, the head of the Cybercrime Unit in the Criminal Investigation Department, the Public Security Directorate is committed to safeguarding Jordan's electronic environment through the continuous monitoring of all social media.

He noted that many complaints had been received about some people claiming to be experts in cybercrimes while they did not represent any official or licensed institution, warning citizens against dealing with them for fear of endangering their lives.

Major Al-Halahla called on fellow citizens, in the event of any complaint or problem, to resort to the Cybercrime Unit and not to resort to such people under any circumstances.

Anyone who falls victim to cybercrime may submit a complaint to the relevant authorities to safeguard themselves from digital threats and blackmail and seek legal redress. To report a cybercrime, a pre-prepared form must be completed and submitted to the Cybercrime Unit, which includes the names and contact information of both the complainant and accused, as well as a description of the offense.

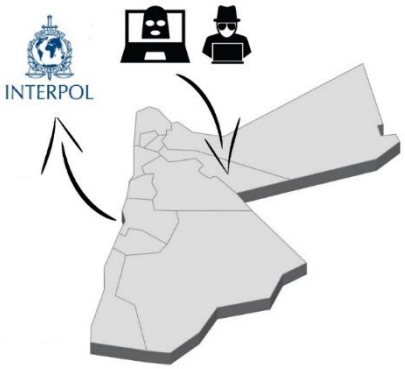
	Form Information and Statement
Form	Date ..... At the Conciliation Penalty Court ..... The complainant (the plaintiff with a personal right) ..... Address ..... The person complained against (the defendants with a personal right)..... Address ..... Content of the complaint ..... Signature of the complainant.....

From the aforementioned information, it can be inferred that the primary obstacles to implementing legal provisions that penalize digital and physical violence against women are protection and reporting mechanisms. The primary reason for this is the reluctance of women to report such incidents, as they often perceive a lack of tangible benefits from doing so. It is essential to ensure that the rights to protection and compensation are afforded to victims of such crimes given that women are the most vulnerable and affected by these heinous acts.[65] To address this issue, it is recommended that the responsibility for investigating and prosecuting such crimes be transferred to the Cybercrime Unit within the Criminal Investigation Department.

The proliferation of the Internet beyond national boundaries and its utilization as a medium for transnational crimes pose significant legal challenges pertaining to the sovereignty of states and the jurisdictional authority of their courts, which are limited to their territorial boundaries. Due to the global nature of cybercrimes, it is essential to establish coordination among domestic laws, international treaties, and cooperative efforts among different nations to effectively combat these crimes. Since 1995, governments worldwide have grappled with a range of issues related to the Internet, including the illegal downloading of copyrighted materials and the dissemination of harmful content that is detrimental to minors.[66]

If the source of a crime is outside of Jordan's territorial boundaries

When a cybercrime occurs in Jordan or affects a resident in Jordan, the provisions of Jordan's Cybercrime Law are nonetheless applicable. If a legal process is initiated and a ruling is issued by a Jordanian criminal court, the pertinent departments of the Public Security Directorate will then reach out to Interpol to track down and apprehend the individuals responsible for these crimes on an international level.



The challenge faced by national criminal courts today is the significant delay between the discovery of new technology violations and the amendment of criminal laws to address them. This process is often slow because of the need to investigate the content of violations in the new technology, identify loopholes in criminal law, and adopt new laws that criminalize computer-related offenses or make appropriate amendments to cybercrime laws. Furthermore, the investigation of potential criminal acts may require equipment and technologies that are not readily available, which adds to the delay in combating internet crimes.

Handling digital evidence poses significant challenges and necessitates specific procedures to safeguard the integrity of information, prevent tampering or erasure of evidence, and respect the rights of innocent Internet users.[67] One of the primary challenges involves identifying the devices and programs used by suspects, uncovering the identities of Internet users through the analysis of electronic communications, recovering erased files, pinpointing evidence related to criminal activity, and decrypting files.

[65] Journalist Hadeel Ghabboun.

[66] Khaled Al-Qudah- digital media expert and member of the Jordanian Journalists Syndicate.

[67] The accused is innocent until proven guilty, and in this regard, entering into the privacy and data of suspects before convicting them means violating their rights. Involvement in a judicial matter does not constitute access to all data.

While the Jordanian judiciary endeavors to effectively implement the individual legislation discussed earlier in adjudicating digital crimes, to safeguard individuals and society from the repercussions of these crimes, there are several obstacles hindering the Jordanian judiciary's ability to do so. One of these challenges is the absence of a precise definition of cybercrime, the complexity of gathering evidence in such cases, and the lack of international collaboration in investigating such crimes. Nevertheless, the Jordanian judiciary remains committed to developing effective mechanisms to implement these treaties and legislation in ruling on cybercrimes, in an effort to shield individuals and society from the negative impacts of these crimes.[68]

The lack of a specific definition of digital or cyber-violence against women is a notable issue. Currently, the Penal Code and cybercrime legal texts refer to offenses, such as defamation, information network usage, and blackmail. Unfortunately, these definitions do not consider the gender approach, despite evidence from numerous studies, including those conducted by the United Nations, which indicates that a significant portion of violence against women is now digital in nature.[69]

The Jordanian judiciary acknowledges the challenges associated with cybercrime and has implemented measures to address this issue. In August 2023, the Cybercrime Law was enacted, and in September of the same year, the Judicial Council announced the allocation of 75 judges and public prosecutors in various specialties to investigate the cybercrimes that the judiciary received.[70] Furthermore, the Jordanian Judicial Institute implemented a training program for judges of the criminal chambers, appellate bodies, and public prosecutors, including two women. The program covered the provisions of the new law, technical and artistic concepts, and the rights of individuals. The council has emphasized its commitment to freedom of opinion and expression and plans to develop a specialized training plan for 2024 that will focus on technical concepts, new systems, criminal aspects, and digital evidence.[71]

[68] Attorney Nidaa Al-Shuwaikh and journalist Hadeel Ghabboun.

[69] Journalist Hadeel Ghabboun.

[70] Jordanian Petra Agency, "The Judicial Council implements a training program on cybercrime law," September 3, 2023.

[71] Facebook page of the Jordanian Judicial Institute, a course for judges entitled (The Best Ways to Implement the Cybercrime Law), October 22, 2023.

Conclusion and Recommendations

The purpose of this paper is to examine the legislative and institutional frameworks governing digital violence against women in Jordan. Through an extensive review of legal texts ranging from the country's constitution and international treaties to relevant laws, including the recently enacted Cybercrime Law, it became evident that the legal system is ineffective in protecting women from digital violence. This is because of the presence of vague provisions, insufficient implementation, and deterrence mechanisms. The feedback provided by experts who were interviewed from various stakeholders in this study further confirmed the need for increased technical, financial, and administrative support for existing tools and resources.

Additionally, there is a need to raise community awareness about the available measures to combat digital violence against women and encourage their utilization. In summary, this study offers general recommendations for addressing digital violence against women in Jordan, followed by specific recommendations for enhancing the legislative and institutional framework in this area.

General recommendations for combating digital violence against women in Jordan:

1. Religious institutions, both Islamic and Christian, should take steps to rectify misconceptions about women and their treatment while simultaneously preserving their dignity and refraining from undermining them. These institutions must also affirm the prohibition of all forms of violence against women as mandated by religious and societal customs.
2. The media play a crucial role in addressing this issue by creating educational programs designed to inform women of their rights and how to access them, as well as educating young men on how to interact with women without causing harm or exposing them to psychological or physical harm. Additionally, the media must emphasize the importance of laws related to digital violence to prevent individuals from engaging in such behavior under the mistaken belief that they are beyond the reach of the law.
3. Governments must also regulate and control discourse on audio-visual communication channels and take measures to address any instances that promote violence in all forms. It is important to highlight the positive aspects of human relations, while condemning all forms of violence.
4. Social and research authorities must conduct thorough analyses and studies on this issue, collecting accurate statistical data on the various forms of violence inflicted on women. These data should be used to develop effective interventions and to continuously update the results of demographic and health surveys. This will enable authorities to monitor trends and evaluate progress in the fight against digital violence against women.

The following recommendations aim to enhance the legal and institutional framework concerning digital violence against women in Jordan:

1. Contact lawmakers gain their support to draft legal texts that provide a comprehensive definition of digital violence against women to counter the potential dangers posed by technological advancements, including blackmail and violence against women. It is crucial to classify digital violence as a criminal offense and include it in the perpetrator's record in case of repetition while ensuring that legislative conflicts do not unfairly benefit perpetrators at the expense of victims. This is an essential aspect of upholding fair trial guarantee.
2. Undertake a comprehensive review of current laws related to cybercrimes, including the Penal Code and the Communications Law, to ensure that gender-based cybercrimes are criminalized and that penalties are intensified in accordance with the National Strategy for Women in Jordan.
3. Lawmakers must continuously revise the laws regulating these spaces to ensure that they provide a safe and secure environment for expression, where women can find protection in the event of any violations.

4. Establish a specialized joint committee focusing on addressing gender-based digital violence. This committee should include representatives from the Cybercrime Unit, judiciary, Ministry of Digital Economy and Entrepreneurship (formerly the Ministry of Communications and Information Technology), Telecommunications Regulatory Authority, National Center for Human Rights (an independent institution by special law), National Committee for Women's Affairs (a specialized civil society institution), and male and female attorneys from civil society and Jordanian Bar Association. The objective is to enhance collaboration in case-level work and to humanize the issue beyond mere plans, policies, and general frameworks.
5. Provide the Cybercrime Unit with adequate support by continuously supplying it with qualified and specialized personnel, maintaining expertise within the unit, and fostering knowledge accumulation. In addition, communication policies and mechanisms between the unit and other relevant government agencies should be established.
6. Train judicial chambers and security agencies dedicated to handling cybercrime cases[72] with the necessary competencies to technically address such offenses and humanize these types of cases.
7. The government must mandate platforms and Internet intermediaries to demonstrate high-level, clear commitments to ensuring women's safety in cyberspace. They should provide straightforward and transparent procedures for reporting and submitting complaints related to digital violence, including on social media platforms, and offer toll-free numbers and services suitable for minors.
8. Engage all relevant entities and institutions, such as telecommunications companies and Internet service providers, to facilitate the reporting and complaint mechanism and collaborate with security and judicial authorities to combat digital violence against women.
9. The Public Security Agency should reveal statistical data on crimes committed by gender. Additionally, annual reports of criminal investigations should provide more information about digital violence against women.
10. The development of a comprehensive law that addresses all forms of violence against women, including those in family, public, and private spaces, is crucial to prioritize the protection, prevention, deterrence, and support of victims of violence, regardless of its form. It is necessary to allocate security and judicial institutions to handle cases of violence against women.

[72] In accordance with the provisions of Article 35 of the Cybercrime Law, No. (17) of 2023.

References

Abdul Mahmoud, Abbas Abu Shama Al-Bashri, Mohammed Al-Amin. (2005). *Domestic Violence in the Age of Globalization* (1st ed.). Riyadh-Saudi Arabia: Center for Studies and Research, Naif Arab University for Security Sciences

Al-Karak Castle Center for Consultations and Training. (2020). Violence Against Women During Elections In Jordan - 2020 Elections

Case No. 114 of the Judicial Year 2001 of the Supreme Constitutional Court "Constitutional."

Ehab Al-Hadri. (2010). *The Alternative Space: The Political and Social Practices of Arab Youth on the Internet*. Giza: The Center for Arab Civilization.

Hanan Abuskin. (n.d.). Hate Speech and Human Rights. Studies in Human Rights.

The Jordanian Judicial Council. (2013). Decision No. 4 of 2013 issued by the Jordanian Constitutional Court.

The Jordanian National Commission for Women. (2020). The National Strategy for Women in Jordan 2020-2025.

The Jordanian National Committee for Women's Affairs. (2022). Study of violence against women in the public and political spheres in Jordan 2022.

Jordanian open-source association.

Mahmoud Abu Farwa Al-Rajabi (2023). Challenges of the Arab Digital Content Industry. Tomorrow.

Mohammed Al-Hamouri. (2009). *Rights and Freedoms between the Whims of Politics and the Requirements of the Constitution* (1st ed.). Dar Wael for Publishing and Distribution.

The Minster of Hashemite Kingdom of Jordan. Jordanian Constitution.

Naji Mohammed Hilal. (2007). *Domestic Violence in Emirati Society: A Field Study* (1st ed.). Sharjah- United Arab Emirates: Police Research Center, Sharjah Police

Noufal Law Office.

Official Gazette. (August 13, 2023). Issue No. 5874. The Minster of Hashemite Kingdom of Jordan.

United Nations Entity for Gender Equality and the Empowerment of Women. (n.d.). Frequently asked questions: Types of violence against women and girls.

UN Women. (2021). Violence against women in the online space: insights from a multi-country study in the Arab States.

WhatsApp Help Centre. About end-to-end encryption.

X Help Centre. (April 2023). Hateful conduct policy.

Interviews with the following experts were conducted as part of this study:

1. Attorney Mohammed Abu Zanad - Member of the Lawyers' Syndicate Council
2. Attorney Nidaa Al-Shuweikh
3. Khaled Al-Qudah – Digital Media Expert, Member of the Jordanian Journalists Syndicate
4. Attorney Lin Al-Khayyat Journalist Hadeel Ghboun
5. Noha Mahrez – Director of Women's Solidarity Institute
6. Dr. Mohammed Moqdadi, Secretary-General of the National Council for Family Affairs.

Appendix: Legal Texts

Constitution

Article (7)

1. Personal freedom is inviolable.
2. Any assault on public rights and freedoms or sanctity of private life for Jordanians is a crime punishable by law.

Article (15)

- The state guarantees freedom of opinion, and every Jordanian has the right to freely express his opinion through speech, writing, photography, and all other means of expression, provided that it does not exceed the limits of the law.
- The state guarantees freedom of scientific research and literary, artistic, cultural, and sports creativity provided that it does not violate the provisions of the law or public order and morals.
- The state guarantees freedom of the press, printing, publishing, and media within the limits of law.
- Newspapers and media may not be disabled, or their licenses may be revoked, except for a judicial order in accordance with the provisions of the law.
- In the event of the declaration of customary or emergency provisions, the law may impose limited control on newspapers, publications, writings, media, and communication on matters related to public safety and national defense purposes.
- This law regulates the method for monitoring newspaper resources.

Article (128)

1. Laws issued under this constitution to regulate rights and freedoms may not affect the essence of these rights or touch on their fundamentals.

Article (19) of the Universal Declaration of Human Rights:

Everyone has the right to freedom of opinion and expression; this includes the freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.

International Covenant on Civil and Political Rights

Article (17)

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor or reputation.

1. Everyone has the right to protect the law against interference or attacks.

Article (19)

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided in paragraph 2 of this article carries special duties and responsibilities. It may, therefore, be subject to certain restrictions, but these shall only be such that are provided by law and are necessary:
    A. Respect for the rights or reputations of others.
    B. Protection of national security or public order (order public), or public health or morals.

Article (20)

1. Any propaganda about war is prohibited by law.
2. Any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence shall be prohibited by law.

Article (26)

All persons are equal before the law and are entitled without any discrimination against equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any grounds such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status.

Convention on the Elimination of All Forms of Discrimination Against Women

Article (2)

State Parties condemn all forms of discrimination against women, agree to pursue by all appropriate means, and without delay, a policy of eliminating discrimination against women and, to this end, undertake:

A. To embody the principle of equality of men and women in their national constitutions or other appropriate legislation if not yet incorporated therein and to ensure, through law and other appropriate means, the practical realization of this principle.
B. To adopt appropriate legislative and other measures, including sanctions where appropriate, prohibits discrimination against women.
C. To establish legal protection of the rights of women on an equal basis with men and to ensure through competent national tribunals and other public institutions the effective protection of women against any act of discrimination.
D. To refrain from engaging in any act or practice of discrimination against women and to ensure that public authorities and institutions act in conformity with this obligation.
E. To take appropriate measures to eliminate discrimination against women by any person, organization, or enterprise.
F. To take appropriate measures, including legislation, to modify or abolish existing laws, regulations, customs, and practices that constitute discrimination against women.
G. Repeat all national penal provisions that constitute discrimination against women.

Article (3)

State Parties shall take all appropriate measures, including legislative measures, in all fields, especially in political, social, economic, and cultural fields, to ensure the full development and progress of women. This is to ensure her exercise of human rights, fundamental freedoms, and enjoyment on an equal basis with men.

Article (5)

State Parties shall take all appropriate measures to achieve the following: (A) Change the social and cultural patterns of behavior of men and women, with a view to achieving the elimination of prejudices and customary and all other practices that are based on the idea of inferiority or the superiority of either of the sexes or on stereotyped roles for men and women.

Article (6)

State Parties shall take all appropriate measures, including legislative measures, to combat all forms of trafficking in women and the sexual exploitation of women.

International Convention on the Elimination of All Forms of Racial Discrimination

Preamble:

The States Parties to this Convention,

Considering that the Charter of the United Nations is based on the principles of dignity and equality inherent in all human beings, and that all Member States have pledged themselves to take joint and separate action, in cooperation with the organization, for the achievement of one of the purposes of the United, which is to promote and encourage universal respect for and observance of human rights and fundamental freedoms for all, without distinction as to race, sex, language, or religion.

The Universal Declaration of Human Rights claims that all human beings are born free and equal in dignity and rights and that everyone is entitled to all the rights and freedoms set out therein, without distinction of any kind, in particular as to race, color, or national origin, considering that all human beings are equal before the law and are entitled to equal protection of the law against any discrimination and against any incitement to discrimination.

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the UN Convention against Transnational Organized Crime

Article (2) – Statement of purpose

The purpose of this protocol is as follows.

A. To prevent and combat trafficking, women and children are receiving particular attention.
B. To protect and assist victims of such trafficking, there is full respect for their human rights.
C. To promote cooperation among state parties to meet these objectives.

Third - Prevention, Cooperation and Other Measures

Article (9) – Anti-trafficking in persons

1. State Parties shall establish comprehensive policies, programs, and other measures:
    A. To prevent and combat trafficking in persons.
    B. To protect victims of trafficking, especially women and children, from further harm.
    C. State Parties shall seek to undertake measures such as research, information, media campaigns, and social and economic initiatives to prevent and combat trafficking in persons.
    D. The policies, programs and other measures established in accordance with this article shall, as appropriate, include cooperation with non-governmental organizations or other relevant organizations and other elements of civil society.
    E. State Parties shall adopt or strengthen measures, including bilateral or multilateral cooperation, to alleviate the factors that make persons, particularly women and children, vulnerable to trafficking, such as poverty, underdevelopment, and lack of equal opportunity.
    F. State Parties shall adopt or strengthen legislative or other measures, such as educational, social, or cultural measures, including bilateral and multilateral cooperation, to deter the demand that fosters all forms of exploitation of persons, especially women and children, which leads to trafficking.

Arab Convention for the Suppression of Information Technology Crimes

Article (6) Crime of Unlawful Entry:

1. Unlawful entry, stay, or any unlawful contact with all or part of information technology or its continuation.
2. The penalty is intensified if this entry, stay, contact, or continuation results in
   A. Erasure, modification, distortion, copying, transfer, or destruction of stored data, electronic devices and systems, and communication networks cause harm to users and beneficiaries.
   B. Obtaining confidential government information.

Article (10)

Crime of Forgery: Anything that involves using information technology to change the truth in the data with the intention of causing harm and with the intention of using them as correct data.

Article (11)

Crime of Fraud: Causing harm to beneficiaries and users intentionally and without right with the intention of fraud to achieve interests and benefits in an illegal way, for the perpetrator or others, by:

1. Introducing, modifying, erasing, or blocking information and data.
2. Interference in the function of operating systems and communication systems or attempts to disable or change them.
3. Disabling devices, programs, and websites.

Article (12) Crime of Pornography:

1. Producing, displaying, distributing, provisioning, publishing, purchasing, selling, or importing pornographic or indecent materials using information technology.
2. The penalty is intensified for crimes related to children and minor pornography.
3. The intensification mentioned in paragraph (2) of this article includes possession of child and minor pornography materials or indecent materials for children and minors on information technology or the storage medium of those technologies.

Article (13)

Other crimes related to pornography: Gambling and sexual exploitation.

Article (14)

Crime of Assault on the Sanctity of Private Life: Assault on the sanctity of private life by means of information technology.

Penal Code

Article (73) Publicity

Publicity means are:

1. Actions and movements if they occur in a public place or a place permissible to the public, exposed to view, or occur in a place that is not one of the mentioned places, but in a way that anyone present in the mentioned places can see.
2. Speech or shouting, whether pronounced or transmitted by mechanical means, is heard in both cases by those who have nothing to do with the act.
3. Writing drawings, manual and solar pictures, films, badges, and images of all kinds if displayed in a public place or a place permissible to the public, exposed to view, sold, offered for sale, distributed to more than one person, or published by electronic means that enable the public to read or view them without restriction.

Article (77)

The partners in the crime committed by the speech transmitted by mechanical means, as stated in the second paragraph of Article (73), or in the crime committed by one of the means mentioned in the third paragraph of the same article are the owner of the speech or writing and the publisher, unless the first proves that the publication was without his consent.

Article (82)

Incitement to commit an offense and interference do not require punishment.

Article (188) Defamation, Slander, and Contempt

1. Defamation: This is the attribution of a specific matter to a person - even in the course of doubt and questioning - that could harm his honor and dignity or expose him to the hatred and contempt of people, whether that matter is a crime that requires punishment.
2. Slander: It is an attack on the dignity of others or their honor or consideration - even in the course of doubt and questioning - without stating a specific matter.

If the name of the victim is not explicitly mentioned when committing the crimes of defamation and slander, or the attributions made were vague, there were indications that there is no doubt with them in attributing those attributions to the victim and in determining their nature. It is then necessary to look at the perpetrator of the act of defamation or slander as if he mentioned the name of the victim, and as if the defamation or slander was explicit in terms of nature.

Article (189)

For defamation or slander to necessitate punishment, it must occur in one of the following forms:

1. Face-to-face defamation or slander, which is required to occur:
   A. In a place facing the victim.
   B. In a place where others (few or many) can hear it.
2. Absentee defamation or slander, and its condition is that it occurs during a meeting with many people gathered or alone.
3. Written defamation or slander and its condition is that it occurs:
   A. What is published and broadcast among people or by what is distributed to a category of people from writings, drawings, satirical pictures, or drafts of drawings (drawings before they are adorned and made).
   B. By what is sent to the victim of open offices (not closed) and postcards.

4. Defamation or slander by means of publications and its condition is that it occurs:
   A. By daily or timed newspapers and magazines.
   B. Any type of publication or media.

Article (190)

Contempt: It is any contempt or insult - other than defamation and slander directed at the victim face-to-face by speech, movements, writing, drawing that were not made public, telegram, telephone, or rough treatment.

Article (306)

Anyone who displays an act contrary to modesty or directs any phrases or makes immoral movements in a way contrary to modesty by saying, acting, moving, or signaling explicitly or implicitly by any means when the assault occurs on:

1. A person who has not completed 18.
2. A male or female person who has completed the eighteenth year of age without consent.

Article (311)

Anyone is punished with imprisonment for one to three years if they:

1. Led or tried to lead a female by threat or intimidation to commit unlawful intercourse in the Kingdom or abroad.
2. Led a female who is not a prostitute or known for moral corruption by false claim or by one of the means of deception to have another person have unlawful intercourse.
3. Handed a female or gave her or caused her to take a drug, substance, or other things intending to sedate her or overcome her so that any person can intercourse with her unlawfully.

Article (319)

Exposure to public morals and ethics: Anyone who is punished with imprisonment for a period not exceeding three months or a fine not exceeding 50 dinars:

1. Sold or acquire with the intention of selling or distributing any obscene material printed, manuscript, solar picture, drawing, model, or any other thing that leads to the corruption of morals, print, or reprint such things and materials in any other way with the intention of selling or distributing them.
2. Displayed in a public place any photography or solar picture or drawing or model obscene or any other thing that may lead to the corruption of morals, or distributed such things to display them in a public place, or
3. Managed or participated in the management of a place that deals with the sale or publication or display of obscene things whether printed or manuscript or solar picture or drawings or models or any other things that may lead to the corruption of morals, or
4. Announced or broadcast by any means that a person deals with the sale of these obscene materials and things, prints them, reprints them, displays them, or distributes them.

Article (348) Repeated

Anyone who violates the privacy of others by eavesdropping or spying by any means, including audio recording, taking pictures, or using a telescope, is punished based on the complaint of the victim with imprisonment for a period of not less than six months and a fine of 200 dinars. The penalty doubles in the case of repetition.

Article (415) (2022 Amendment)

1. Everyone who threatened a person to expose a matter or disclose it or news about it and was capable of affecting the value of this person or his honor or the value of one of his relatives or his honor is punished with imprisonment from three months to two years and a fine from fifty dinars to two hundred dinars.
2. Everyone who blackmailed a person to carry him to bring an illegal benefit to him or others is punished with imprisonment for a period not less than three months and a fine not less than fifty dinars and not exceeding two hundred dinars.
3. Everyone who blackmailed a person to carry him to bring an illegal benefit to him or others by claiming a traffic accident, even if his act did not imply a threat or was not capable of undermining the value of this person or his honor or the honor of one of his relatives is punished with imprisonment for two years and a fine of (50) dinars, and the punishment will be imprisonment for a period not exceeding one year if the purpose of claiming the accident was merely to harm others.

Communications Law

Article (56)

Phone calls and private communication are considered confidential matters that may not be violated under the penalty of legal liability.

Penalties for directing illegal messages:

Article (75)

A. Everyone who proceeds by any means of communication to direct threatening messages, insults, or messages contrary to morals or transmitted fabricated news with the intention of causing panic is punished with imprisonment for a period not less than a month and not exceeding a year or a fine not less than (300) dinars and not exceeding (2000) dinars or both penalties.
B. Everyone who carried out or contributed to providing communications services in violation of public order or public morals is punished with the penalties stipulated in paragraph (a) of this article, in addition to the application of the provisions stipulated in Article (40) of this law.

Penalty for obstruction or deletion of message contents

Article (76)

Everyone who intercepted, obstructed, distorted, or deleted the contents of a message by means of communications networks or encouraged others to do this work is punished with imprisonment for a period not less than a month and not exceeding six months, a fine not exceeding (200) dinars, or both penalties.

Cybercrime Law

Article (6)

Any individual who intentionally enters, publishes, or uses a program or a programming command through the information network or an information technology tool or by using an information system to cancel, delete, add, destroy, disclose, damage, block, encrypt, modify, change, transfer, copy, capture, or enable others to access data or information or obstruct, disrupt, stop, or disable the operation of the information system or access to it or change a website or cancel it or damage it or modify its contents or occupy it without permission or in a way that exceeds or violates that permission or impersonates its character or impersonates the owner's personality shall be punished with imprisonment for a period not less than six months and a fine not less than (2500) two thousand and five hundred dinars and not exceeding (10000) ten thousand dinars.

Article (7)

A. Any individual who intentionally and without right intercepts the path of data, captures its content, obstructs, distorts, deletes, or records that content whether sent through the information network, information technology, information system, data exchanged within the system, or the same network shall be punished with imprisonment for a period not less than six months and a fine not less than (1500) one thousand and five hundred dinars and not exceeding (6000) six thousand dinars.
B. The perpetrator is punished with imprisonment for a period not less than one year, a fine not less than (3000) three thousand dinars and not exceeding (6000) six thousand dinars if he discloses or leaks or uses what he obtained through interception.
C. If interception occurred on information, data, or any communication for an official body, the penalty is temporary work for a period not less than five years and a fine not less than (15000) fifteen thousand dinars and not exceeding (45000) forty-five thousand dinars.

Article (13) - Paragraph A

1. Any individual who sent, published, prepared, produced, saved, processed, displayed, printed, bought, sold, transferred, or promoted activities or works of pornography using the information network, information technology, information system, or website shall be punished with imprisonment for a period of not less than six months or a fine of not less than (3000) three thousand dinars and not exceeding (6000) six thousand dinars.
2. Prosecution is carried out in the crimes stipulated in item (1) of this paragraph based on the complaint of the victim who has completed the eighteenth year of age, and the public rights lawsuit is dropped by the victim's pardon.
3. If the purpose of the acts stipulated in item (1) of this paragraph is to guide or incite to commit a crime or with the intention of sexual exploitation, it is pursued without the need for a complaint, and the penalty is imprisonment for a period not less than one year and a fine not less than (6000) six thousand dinars and not exceeding (15000) fifteen thousand dinars.

Article (14) - Paragraph A

A. Any individual who used the information network, information technology, or information system or created a website to facilitate, promote, incite, assist, or encourage prostitution and immorality or to seduce another person or to expose public morals shall be punished with imprisonment for a period not less than six months and a fine not less than (9000) nine thousand dinars and not exceeding (15000) fifteen thousand dinars.
B. Any individual who used the information network, information technology, or information system or created a website for the purposes stipulated in paragraph (A) of this article to exploit someone who has not completed the eighteenth year of age or who is suffering from a mental illness or mental disability in prostitution shall be punished with temporary work and a fine of not less than (15000) fifteen thousand dinars and not exceeding (45000) forty-five thousand dinars.

Article (15) - Paragraph A

Any individual who intentionally sent, re-sent, published data, or information through the information network, information technology, information system, website, or social media platforms that includes false news or defamation or slander or contempt of any person shall be punished with imprisonment for a period not less than three months and a fine of not less than (20000) twenty thousand dinars and not exceeding (40000) forty thousand dinars.

Although the definition of "false news" did not appear in the law, but "false news" appeared in the Penal Code articles from 130 to 132, which is related to undermining the state and affecting the nation's psyche with weakness and "fabricated news" appeared in the Communications Law Article 75.

Article (17)

Any individual who intentionally uses the information network, information technology, information system, website, or social media platform to publish what could stir up sedition or feuds, undermine national unity, incite hatred, call for violence, justify it, or insult religions shall be punished with imprisonment from one year to three years and a fine not less than (5000) five thousand dinars and not exceeding (20000) twenty thousand dinars.

Article (19)

A. Any individual who uses an information network, technology, information system, website, or social media platform to publish a recording, picture, or video of what the person is keen to preserve and not show or conceal from the public with the intention of defamation or insult or obtaining any personal gain – even if they obtain those pictures, recordings, or videos legitimately – shall be punished with imprisonment for a minimum of three months and a fine ranging from 20000) twenty thousand dinars to (40000) forty thousand dinars.
B. Any individual who anyone who used an information network or information technology or information system or a website or social media platform to carry out installation or modification or processing on a recording or picture or scene or video of what the person is keen to preserve and not show to the public with the intention of defamation or insult or obtaining a benefit shall be punished with imprisonment for a minimum of than two years and a fine ranging from (25000) twenty-five thousand dinars to (50000) fifty thousand dinars.

Article (20)

Anyone who asks or accepts for himself or for others a gift, promise, or any other benefit whether this was done inside the kingdom or outside it when they publish or re-publish illegal content or false news, using an information network, information technology, information system, website, or social media platform shall be punished with imprisonment for a minimum of one year to three years and a fine equal to the value of what was requested or accepted in cash or kind provided that it is not less than (5000) five thousand dinars.

Article (26)

Anyone who commits any crime punishable under any legislation using the information network, information technology, information system, website, participate ind, intervened, or committed to commit it shall be punished with the penalty stipulated in the legislation.

Article (27)

Anyone who intentionally participates, intervenes, or incites committing any of the crimes stipulated in this law shall be punished with the penalty specified in it for its perpetrators.

Article (28)

The penalties stipulated in this law are doubled in the following cases:

A. If the criminal commits his crime by exploiting his job, work, or his granted powers.
B. If there are multiple victims.
C. If the commission of any of the crimes stipulated in this law is repeated.
D. If the criminal commits his crime to the benefit of a foreign country or an illegal organization.

Article (30)

The application of the penalties stipulated in this law does not prevent the ruling of any harsher penalties stipulated in any other law.

Article (33)

A. When the information system, website, or service provider inside or outside the kingdom, social media platforms, or the person responsible for any account, public page, public group, channel, or its equivalent publish any materials in violation of the provisions of this law or any other applicable legislation in the kingdom, the competent public prosecutor or court must issue an order to those in charge to take the following actions:
    1. Remove, block, stop, disable, record, or intercept the path of data or any post or content, prevent access to it, or block the user or publisher temporarily during the period specified in the decision.
    2. Provide the involved court with all the data or information necessary to reveal the truth, including the data of the owner or user of the website or information system that helps in identifying him and conducting legal prosecution.
    3. The urgent preservation of the data and information is necessary to reveal the truth, store it, and maintain its integrity.
    4. Maintaining confidentiality.
B. In the case of non-response or refusal of those in charge of the information system, social media platform, website, or service provider to the order stipulated in item (1) of paragraph (A) of this article, or if speed requires it, it is permissible for the competent public prosecutor or the competent court and with a reasoned decision to issue an order to the competent authorities to ban the information system, the website, social media platform, or the service from the national network or block access to the violating content.
C. A fine ranging from (15000) fifteen thousand dinars to (30000) thirty thousand dinars or both of these penalties is imposed on anyone who refrains from implementing or violating the orders of the public prosecutor or the competent court.

Article (37)

A. Social media platforms outside the kingdom, which have a number of subscribers exceeding one hundred thousand subscribers in the kingdom, must establish an office for them inside the kingdom to deal with requests and notifications issued by judicial and official bodies.
B. In the case of non-compliance by social media platforms outside the Kingdom with what is stated in paragraph (A) of this article, these platforms are notified by the Communications Regulatory Authority of the need to comply with the above statement within a timeframe of six months from the date of notification.
C. If the period stipulated in paragraph (B) of this article has expired and social media platforms outside the Kingdom have not complied with what is stated in paragraph (A) of this article, the Communications Regulatory Authority has the right to take the following measures in succession:
    1. Ban advertisements on these platforms in the Kingdom for a period of (60) sixty days.
    2. If the period stipulated in item (1) has expired, the bandwidth of Internet traffic is reduced by (25%) on these platforms for a period of (60) sixty days.
    3. If the period stipulated in item (2) has expired, the bandwidth of Internet traffic is reduced by (50%) on these platforms for a period of (60) sixty days.
    4. If the period stipulated in item (3) has expired, the bandwidth of Internet traffic is reduced by (75%) on these platforms for a period of (60) sixty days.

Article (38)

A public right lawsuit and a personal right lawsuit are filed against the accused before the competent judicial reference if any of the crimes stipulated in this law are committed using the information network, information technology, information system, social media platforms, websites, or any electronic publishing means inside the kingdom, or committed outside the kingdom and caused damage to any of its interests, its citizens, or residents, or the effects of the crime occurring in it wholly or partially.

Civil Law

Article (54)

Anything that can be physically or morally possessed and benefited from it legally and does not go out of dealing by its nature or by law is valid as a place for financial rights.

Article (62)

There should be no harm to malice.

Article (71)

1. Moral rights are due to something immaterial.
2. The provisions of special laws shall be followed with respect to the rights of the author, inventor, artist, trademarks, and all other moral rights.

Article (256)

Any harm caused to others obliges the perpetrator, even if not discerning, to guarantee harm.

Article (257)

1. Damage is either a direct or an indirect cause.
2. If harm occurs directly, the guarantee is obligatory without any condition. However, if it occurs due to causation, conditions such as trespass, intention, or the act leading to harm are required.

Article (258)

If direct and indirect causes coincide, the judgment is attributed to the direct cause.

Article (259)

If someone deceived another within the damage that resulted from that deception.

Article (265)

If multiple individuals are responsible for a harmful act, each of them is liable in proportion to their share, and the court may decide either equally, jointly, or severally among them.

Article (267)

Legal provisions address moral damage. Anyone who infringes upon another person's freedom, dignity, honor, reputation, social standing, or financial status is held responsible for the resulting moral harm.

Article (279)

1. What you have taken is that you are obliged to return.
2. Whoever usurped the money of others, they must return it to the state it was in at the time of usurpation and in the place of usurpation.
3. If anyone consumes, damages, loses, or destroys something, whether intentionally or unintentionally, they are liable for its equivalent value on the day of the wrongful act and at its location of the wrongful act.
4. They also guarantee both benefits and profits.

Article (280)

If someone damages the property that has been wrongfully taken from them by the usurper, the rightful owner has the option to either reclaim it from the usurper or seek compensation from the person who caused the damage. The choice lies in the rightful owner, and the person who caused the damage cannot reclaim it from the usurper.

Article (281)

If the usurper disposes of the wrongfully taken property through exchange or donation, and the usurped property is damaged in whole or in part, while in the possession of the person to whom the usurper disposed of it, the rightful owner has the option to either reclaim it from the usurper or seek compensation from the person who caused the damage. The choice lies with the rightful owner, and the person who caused the damage cannot reclaim it from the usurper, according to the provisions of the law.

The Protection from Domestic Violence Law, No. (15) of 2017

Article (2)

Domestic violence: Crimes committed by one of the family members against any of its members.

Personal Status Law, No. (15) of 2019

Article (126)

Either spouse may request divorce due to conflict or discord if they claim harm inflicted upon them by the other party, making it impossible to continue the marital relationship. This harm can be physical, such as actual or verbal abuse, or psychological, encompassing any reprehensible behavior or violation of good morals. Additionally, the insistence of the other party on neglecting marital duties and rights, as referred to in the third section of the third chapter, constitutes psychological harm.

Electronic Transactions Law, No. (15) of 2015

Article (24)

Any person shall be subject to a penalty of imprisonment for a period no less than three months and no more than three years or a fine of no less than (1000 JD) one thousand Jordanian Dinar and no more than (5000 JD) five thousand Jordanian Dinar or by both penalties if he/ she:

A. Establishes, publishes, or submits an electronic authentication certificate for an illegal or fraudulent objective.
B. Provides a party engaged in electronic authentication with faulty information under the intent of issuing, invalidating, or canceling an authentication certificate.