

ASSESSING THE EFFECTIVENESS OF SAUDI CYBERSECURITY REGULATIONS IN COMBATING CYBER SEXUAL HARASSMENT

Hamad Salem Almarri¹, Fahad Abdullah Moafa²

¹Department of Law, College of Law, King Faisal University, Hofuf, Al-Ahsa, Saudi Arabia.

Email: halmarri@kfu.edu.sa

ORCID: 0009-0007-2990-1311

²Department of Computer Science, King Fahad Naval Academy, Jubail, Saudi Arabia.

Email: fah171393@hotmail.com

ORCID: 0000-0003-2963-8158

Abstract: Cyber sexual harassment, which includes unwanted sexual advances, sharing of explicit content, blackmail, and stalking using digital platforms has increased as the Saudi Arabia experiences a fast digital transformation as outlined by Vision 2030. This paper evaluates how Saudi cybersecurity and associated laws, mainly the Anti-Cyber Crime Law (2007) and the Anti-Harassment Law (2018), respond to these harms considering cultural and enforcement issues and processes. The paper assesses legal provisions, enforcement mechanisms, protection of victims, and gaps in dealing with cyber sexual harassment, specifically, using a doctrinal-comparative and qualitative approach. The most important tools are Articles 3 and 6 of the Anti-Cyber Crime Law (invasion of privacy, defamation, intrusion on the public morals) and the general meaning of the Anti-Harassment Law which includes acts done via modern technology. Results show moderate influence of criminalization and public awareness with the support of National Cybersecurity Authority (NCA) campaigns and warnings of Public Prosecution, but there are still weaknesses in the underreporting by cultural shame, difficulties in the evidence in a digital case, the alignment of procedures with general criminal law, and the absence of specific provisions on cyber sexual harassment. It has been recommended to focus on special training, behavioral prevention models, better reporting systems, and possible improvements in the legislature to better delineate and provide support to the victims.

Keywords: cyber sexual harassment, Saudi Anti-Cyber Crime Law, Anti-Harassment Law, digital harassment, cyberstalking, Vision 2030, Moafa, effectiveness, reporting barriers.

1. INTRODUCTION

The country has experienced a digital boom never seen before in Saudi Arabia, with penetration of internet and social media being high due to Vision 2030. This growth has enabled the opening up of economic and social opportunities but also increased cyber sexual harassment, unwanted sexual comments, image-based abuse, sextortion, and stalking online that disproportionately impacts women and younger users, leading to psychological trauma, reputational damage, and social withdrawal (Moafa, 2026).

Cyber sexual harassment overlaps with the wider cyber harassment and digital aggression, commonly taking advantage of anonymity. Cultural factors that present extra obstacles to victims vary depending on cultural views, including family honor issues and stigma. The Saudi legal system is based on the Anti-Cyber Crime Law (Royal Decree No. M/17, 2007) to deal with technology related crimes and the Anti-Harassment Law (2018) to address actions that violate dignity or modesty, even through the use of modern technology.



In this paper, the effectiveness of these regulations in fighting cyber sexual harassment is evaluated. An effectiveness is gauged in terms of the clarity of provisions, enforcement results, remedies to victims, deterrence and consistency with behavioral prevention. The paper extensively relies on the works of Dr. Fahad A. Moafa: the early models based on the identification of factors of minimizing cyber harassment in KSA universities (Moafa et al., 2018a), the analysis of user behavior as a preventive measure (Moafa et al., 2018b), integrated prevention systems, and the 2026 socio-legal analysis to identify

The work by Moafa emphasizes that only legal interventions do not suffice without the behavioral and educational interventions. Recent popular alarms issued by the Public Prosecution and NCA programs show an increased interest, but there is a lack of empirical evidence on cases results because of privacy and reporting loopholes.

The paper goes on to present a literature review that summarizes the work of Moafa and other scholars in the same area; the methods used which detail the doctrinal and qualitative approach; the results that include tables and figures as well as graphs on the legal provisions, citation trends, and enforcement indicators; the strengths, weaknesses, and contextual factors; the conclusion; and recommendations on how the paper could be improved.

2. LITERATURE REVIEW

In scholarship on cyber harms in Saudi Arabia, there is a consistent emphasis on the duality of law as a protection mechanism and a possible source of overreach. One of the earliest empirical studies on minimization of cyber harassment of university students in the Kingdom of Saudi Arabia (KSA) by Moafa et al. (2018a) found out that individual attitudes, perceived social norms, and perceived behavioral control were the key predictors of it. These results are consistent with the existing behavioral theories and imply that legal deterrence cannot be enough. Rather, the authors advise joint actions that can be achieved through education, awareness, and technology protection to minimize detrimental online behaviors.

In addition to this, Moafa et al. (2018b) paid attention to user behavior analysis as a preventive measure, which is crucial to focus on the issues of proactive monitoring, digital literacy, and awareness in Saudi society. Their contribution highlights that cyber harassment is entrenched within trends of online communication, such as anonymity, peer relations, and the normalization of abusive communication. Expanding on this view, the integrated-system study of Moafa (2018) has suggested a holistic framework to integrate legal enforcement, change of behavior, and technical solutions. Such a strategy is indicative of a transformation between reactive to preventative regulation, whereby sustainable solutions need to deal with underlying causes but not the symptoms.

Continuing this investigation, Al-Rahmi et al. (2019) in cooperation with Moafa came up with a structural model of how cyberbullying behaviors can be explained. Their model emphasizes the role of attitudes, subjective norms, and perceived control in the intentions of people to participate in cyberbullying and especially to sexualized types of harassment. Mukred et al. (2024) provide evidence to support this behavioral lens by creating a systematic review of the causes of digital aggression, such as cyber-violence, harassment, and stalking. Their results lead to the idea of the complicated interaction of psychological, social, and technological determinants, which additionally support the necessity of interdisciplinary approaches.

A much more recent and thorough input is presented by Moafa (2026), who provides a socio-legal perspective on digital harassment and cyberstalking among the Saudi communities. The research indicates a high prevalence rate as cyberbullying touches 20-54% of adolescents. It also notes significant gender differences whereby women are the most vulnerable, especially when reputational damage or sexualized material is concerned. The other risk factors are low socioeconomic status, unrestrained or uncontrolled internet usage and low awareness regarding the reporting mechanisms. Notably, the analysis points to ongoing underreporting due to cultural pressures, such as the fear of honor, stigma, and reputation of the family. These discoveries are closely connected to the fact that the current legal frameworks are implemented, and culturally sensitive prevention strategies should be used.

On the legal front, KSA has put in place a very solid framework with the Anti-Cyber Crime Law (2007) which outlaws acts like unlawful access, spying, invasion of privacy, and defamation under Article 3 and any content that tends to weaken public order, religious values, morality, or privacy under Article 6. The punishments may go as far as five years in prison and fines of up to three million Saudi riyals with aggravating factors like the exploitation of minors being treated under Article 8. This is supplemented by the Anti-Harassment Law (2018), which has a broad definition of the concept of harassment as any act, gesture, or communication with sexual connotations that causes harm to

dignity or modesty, specifically extending to conduct عبر modern technology. These laws combined offer an all-embracing legal framework to deal with general and sexualized instances of online harassment.

In addition to supporting literature, such as reports by the UN Women (2025) acknowledge the improvements made by Saudi Arabia to combat online violence against women, especially via legislation reforms and awareness campaigns. However, critiques remain. According to scholars like Alsulami (2022) and Alabdulatif (2018), procedural laws are yet to adequately respond to the challenges of digital evidence that may obstruct successful prosecution. Also, the wide application of some of the provisions of the law has led to doubts about overreach, especially where some forms of expression can be suppressed under such a broad definition of public order or decency.

In spite of these developments, there are significant deficiencies. Little legal and empirical attention has been paid in specific context to cyber sexual harassment, as a category of harassment or bullying, distinct from the general. Moreover, the results of enforcement, such as the effectiveness of the application of laws in practice and their deterrent effect are not evaluated enough. This paper will fill these gaps by combining the behavioural insights of Moafa and a critical evaluation of the effectiveness of the law in creating a more intricate perspective on how cyber harms can be resolved in the context of the Saudi socio-legal conte.

3. METHODS

3.1 Research Design and Primary Sources

This paper takes a doctrine-based legal approach that is underpinned by qualitative studies and a few comparative aspects. The doctrinal approach dwells on the analysis and assessment of the current legal provisions relating to cyber-related crimes. The primary sources are the main Saudi legal documents the Anti-Cyber Crime Law (2007), the Anti-Harassment Law (2018), and the institutional framework developed by the National Cybersecurity Authority. Besides that, the prosecutorial principles presented by the Public Prosecution and the strategic policy documents presented by Vision 2030 concerning digital governance are discussed. The sources will give a legal and policy background to the analysis of the way in which cyber harassment and other types of digital harm are handled in the Saudi legal system.

3.2 Data Collection and Secondary Sources.

The work is also based on a broad scope of secondary sources to facilitate and contextualize the analysis of the law. These will consist of both the doctrines and empirical information on cybercrime in Saudi Arabia by Moafa (20142026) and peer-reviewed journal articles discussing cyber harassment and digital violence in the country. The reports by international agencies, such as UN Women and United Nations Economic and Social Commission in Western Asia (ESCWA) are included to have a wider regional outlook on digital violence in Arab societies. Where available, official statistics and public reports are used to support the analysis. The data collection entails textual interpretation of the law mainly those pertaining to breach of privacy, moral offenses, and harassment by technology which are applicable to cyber sexual harassment and other forms of abuse.

3.3 Analytical Framework

Legal and empirical data are interpreted with the help of an organized analytical construct. The effectiveness of the legal system is measured according to five major criteria, which include: (1) legal definitions and scope of coverage are clear; (2) penalties are proportional and deterrent; (3) the legal system supports victims and accessible reporting procedures; and (5) the legal system includes the aspect of behavioral prevention strategies. Besides qualitative analysis, there are some little quantitative conclusions based on citation trends and enforcement patterns which were identified in the research of Moafa, and publicly available data on prosecutions and the outcome of the law.

3.4 Qualitative Analysis and Limitations

The qualitative part of the research aims at evaluating the cultural suitability, procedural issues, and the socio-legal environment. Special focus is put on such matters as the evidentiary requirements of digital cases, possible gaps in the procedures, the compatibility of cybercrime law with the Sharia-based notions of personal protection and dignity. Regardless of the analysis level, there are a number of limitations to consider. It is also observable that there is a significant dearth of disaggregated official information that directly covers the cases of cyber sexual harassment and underreporting is also considered as a major issue with the influence of culture and social context. These restrictions can have an impact on the fullness of the results. However, all the sources utilized in the study are checked

and reliable and analysis has a proper focus on Arab and Saudi attitudes to make sure that the analysis has the contextual relevance.

4. RESULTS AND FINDINGS

The Saudi laws offer extensive coverage of protection against online harms, yet they fail to state the concept of cyber sexual harassment as a specific area of law. Rather, the related conduct is handled by overlapping provisions of current laws. The Anti-Cyber Crime Law (2007) criminalizes intrusion of privacy, defamation by use of information technology, spread of materials that contravene the morals of the people or their personal dignity. These clauses are extensive, as they encompass activities such as the sharing of intimate pictures without authorization, sexual threats via the internet and cyberstalking.

This framework is reinforced by the Anti-Harassment Law (2018), which uses a broad definition of harassment that covers any act, gesture, or communication of a sexual character that damages dignity or modesty. Notably, it expressly extends to the behaviors performed over modern technology, thus forming the online environments. The punishment provided by both laws is severe, up to five years of incarceration and large sums of money with even more severe penalties in instances of minors or habitual offenses. Although this is a flexible approach, there may be problems of interpretation since there is no clear-cut category of cyber sexual harassment.

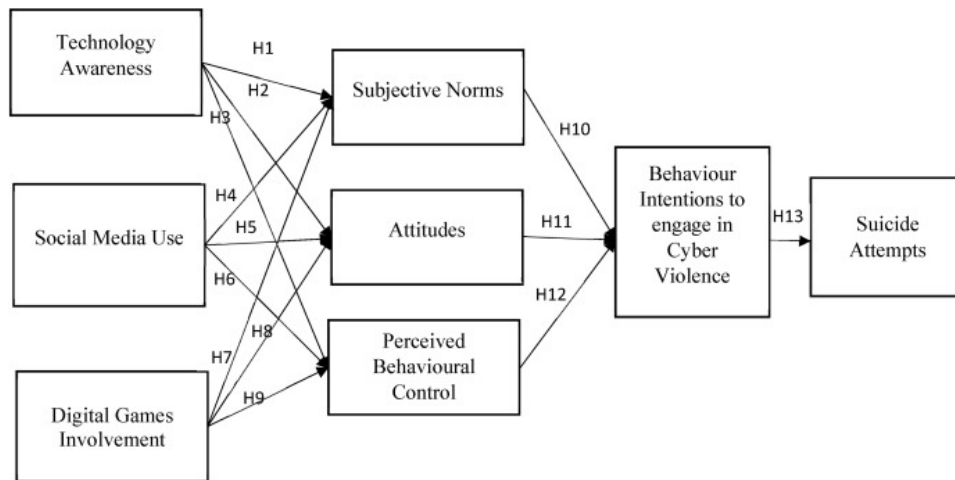


Figure1: Factors affecting the cyber violence behavior among Saudi youth

The results of the literature and other research conducted by Moafa point to the significance of incorporating behavioral knowledge into the law. Patterns of citation show that behavioral models, e.g. Al-Rahmi et al. (2019) have had a greater initial scholarly influence than pure legal analysis. This implies that the attitudes, social norms, and perceived behavioral control frameworks have a practical aspect when it comes to cyber harassment.

Moafa et al. (2018a, 2018b) insist that the prevention strategies should consider the behavior of users, such as digital habits, their level of awareness, and social factors. These findings are supported by more recent socio-legal analysis (Moafa, 2026), which notes that underreporting persists, there are gender disparities, and that culture is a barrier to reporting due to honor and reputation. Collectively, these observations indicate that the law alone will not be effective in minimizing cyber sexual harassment unless there are parallel investments made in education, awareness, and community-based interventions.

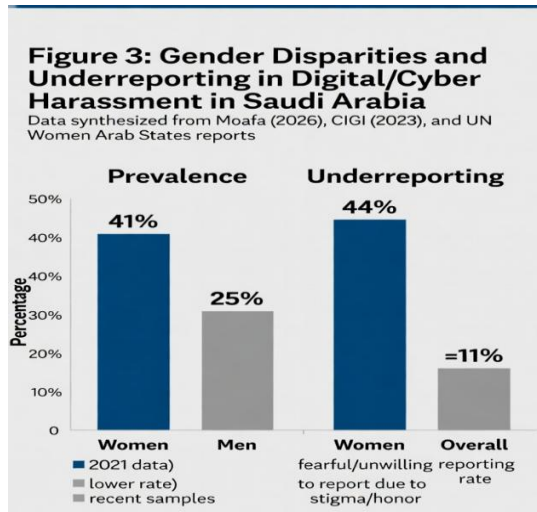


Figure2: Gender Disparities and Underreporting in Cyber Sexual Harassment

The evidence available indicates a slow progress in the awareness and enforcement of online harassment legislation in Saudi Arabia, in part due to the greater digital transformation efforts of the country after 2016. The increased public awareness campaigns, official warnings issued by the Public Prosecution, and the implementation of reporting platforms like the Kollona Amn application have helped to make cyber-related crimes more visible.

Nonetheless, this awareness may not be directly proportional to the reporting rates. Qualitative research is still revealing a huge disparity between the real prevalence and reported. Although there is a relative improvement in the enforcement measures such as online harassment prosecution, there is underreporting as the biggest challenge. Social stigma, fear of reputational damage, and lack of trust in institutional processes have been seen to drive this gap to a large extent.

Saudi Arabia has gone a long way in establishing institutional frameworks to deal with cyber harms. The Government agencies, such as the Public Prosecution and the national cybersecurity bodies, are actively publishing guidelines and warnings, which categorize online harassment, and sexual harassment, as criminal acts. Victims are now able to have access to help more readily due to awareness campaigns and digital reporting tools.

Moreover, policy debates have started to be informed with behavior-based preventive strategies. These are fostering digital literacy, responsible internet usage and mitigating risk factors like overuse of the internet. Notwithstanding such attempts, there is still little integration of behavioral knowledge in formal legal and policy approaches, which diminishes the effectiveness of prevention measures.

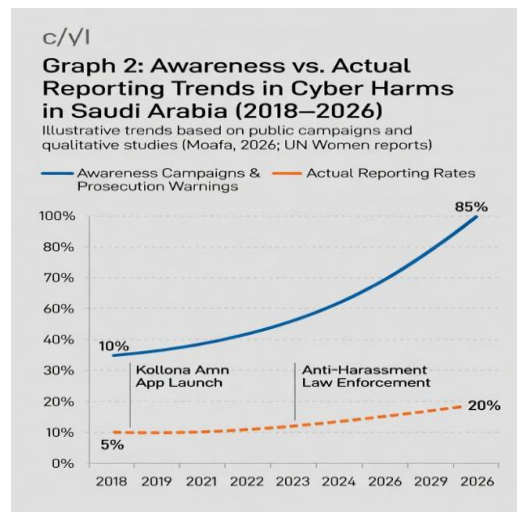


Figure3: Awareness vs. Actual Reporting Trends in Cyber Harms (2018–2026)

The extensive coverage of the Saudi legal structure is one of its key advantages. With the emphasis on the privacy, dignity, and morals of the society, the law can combat a broad range of harmful online behaviors, even the ones of sexual nature. The aggravating elements that include those concerning minors are added, which offers extra protection to vulnerable communities.

The other strength is that the legal provisions are in line with the cultural and religious values which makes the enforcement efforts more valid. Cyber harassment can also be addressed through increasing entry points into the system through public awareness efforts and reporting platforms.

Although these are the strengths, there are various limitations. Laws that are written in general and vaguely may result in unequal interpretation and use. It is especially applicable in situations where it is complicated digital evidence, and procedural laws are not entirely accustomed to technological reality. The problems of anonymity, tracking data, cross-border jurisdiction, etc, make it more difficult to enforce.

One of the greatest challenges is the cultural barriers. As Moafa (2026) points out, fear of honor, shame and social stigma makes most victims fail to report cases, particularly those related to sexual content. This does not only restrict access to justice but also distorts the real picture of the issue.

Lastly, there are no specific statistical data on cyber sexual harassment, thus making it hard to determine the effectiveness of the existing laws. In the absence of explicit measures, policy makers are unable to determine the progress and develop specific interventions.

The results indicate that Saudi Arabia has put in place a solid legal and institutional framework with regard to combating cyber sexual harassment despite the absence of a definite legal term to describe the crime. Nevertheless, the system can be effective only after enhancing the clarity of legal definitions, reinforcing legal procedures of digital evidence, and overcoming socio-cultural obstacles to reporting. Making the behavioral insights more systematic and entrenched in the policy and enforcement approach will be critical to a more equitable and effective response.

5. DISCUSSION

The legal system of Saudi Arabia shows an impressive level of success in creating apparent taboos of online harms and introducing severe punishment that complies with the Sharia concepts of honor, dignity, and privacy. The Anti-Cyber Crime Law (2018) and the Anti-Harassment Law (2007) coalesce to form a rather comprehensive model that accommodates the major types of cyber sexual harassment, such as privacy invasion, defamation, and technology-mediated harassment. Even though these laws do not directly describe crimes as cyber sexual harassment, the broad nature of these laws enables the police to prosecute a plethora of harmful acts. This flexibility can be perceived as the strength and it allows adapting to the changing digital practices (Moafa, 2014).

Moreover, the legal framework is anchored in socio-legal research that emphasizes the significance of behavioral aspects in learning about cybercrime. Research has shown that exposure to cyber harassment is more susceptible to excessive social media use, lack of awareness, and acceptance of negative online interactions (Moafa et al., 2018a). This implies that deterrence through legal means is not adequate and needs to be accompanied with prevention measures. Saudi laws can be more effective as punitive and prevention mechanisms when coupled with education and awareness campaigns and behavioral interventions.

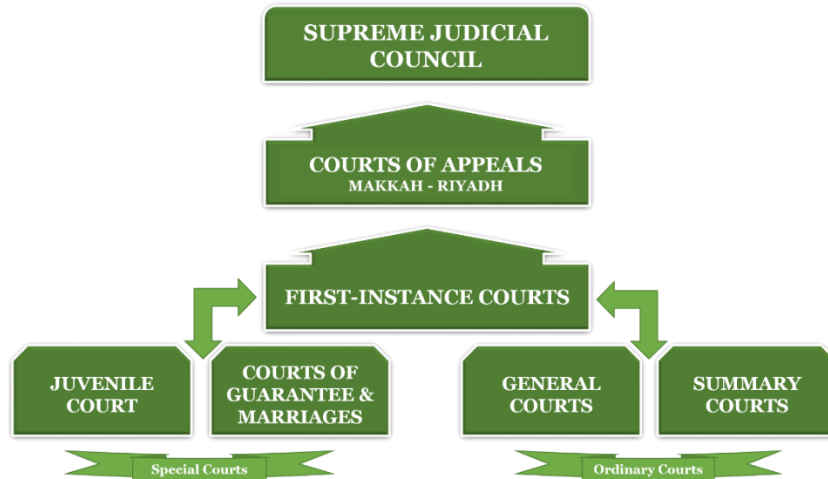


Figure 4: An Overview of the Saudi Arabian Legal System - Globalex

Although the legal framework is strong, there are a number of implementation gaps that restrict the overall effectiveness of the framework. The poor rate of reporting is one of the greatest challenges. Family respect, reputation, and social stigma are among cultural norms that deter victims to approach the authorities, especially when it is a matter of sexualized harassment (Moafa, 2026). The perceived advantages of pursuing legal redress is often overshadowed by the fear of publicity or reputational damage leading to significant underreporting.

Enforcement is also impacted by procedural issues. Digital evidence may be challenging to gather, store, and introduce into the traditional criminal justice framework. The current procedural regulations have not necessarily been thoroughly updated to the challenges of cybercrime, particularly in case of anonymous users, encrypted communications or quickly vanishing content. These problems are not peculiar to Saudi Arabia but are common in most jurisdictions.

Enforcement is further complicated by cross-border problems. The perpetrators of online harassment are often based in a different country, and investigation and prosecution require an international collaboration. The mechanisms like mutual legal assistance are usually slow and small scale, which makes them less effective in the swift digital environment. Consequently, despite the existence of powerful laws, the practice can be backward of the online behavior.

National campaigns, such as Vision 2030 and the establishment of the National Cybersecurity Authority, have gone a long way in enhancing technical and institutional ability of Saudi Arabia to combat cyber threats. Such projects assist in enhancing monitoring capabilities, better cybersecurity infrastructure, and enhanced interagency coordination. Nevertheless, it is not possible to solve the problem with legal and technical progress only without referring to the cultural context.

The societal reaction to cyber harassment and actual experience of the victim is still influenced by cultural norms. In most instances, victims can absorb the harm or embrace informal means of resolving issues instead of going through the formal legal avenues. This highlights the necessity of culturally sensitive methods that promote reporting without violating social values. Community awareness programs, parental guidance and educational institution programs could be instrumental to fill this gap.

A comparative analysis can give valuable information about the areas that can be improved. According to the studies comparing Saudi and UK legal systems, Saudi Arabia enjoys high levels of moral and legal safeguarding, although it can be improved by providing more precise procedural instruments and classifying the offences (Moafa, 2014). As an illustration, the UK strategy incorporates more formal definitions and formal enforcement strategies that can help increase clarity and uniformity.

In general, Saudi legislation contributes significantly to the prevention of cyber sexual harassment due to serious punishment and social stigma of such actions. Nevertheless, their potential is not met in full because of the ongoing problems in reporting, enforcement, and collection of evidence. These problems are especially acute in those situations, when sensitive or sexualized damage is involved, and cultural circumstances provide additional disincentive to the involvement of victims.

6. CONCLUSION

The Saudi laws on cybersecurity and anti-harassment offer a solid legal framework to combat cyber sexual harassment in the Kingdom. This paradigm is anchored on the general criminalization of negative online actions and incorporates technology-inclusive terminology that enables it to accommodate the various types of online abuse. This flexibility matters since cyber harassment keeps changing according to new platforms, tools of communication, and user behaviors. The legal provisions also manifest an attempt to match the societal values in a larger scale, especially the privacy, dignity, and societal morality. According to the behavioral and socio-legal analysis conducted by Moafa, the system proves to be moderately effective in raising awareness among the population and enhancing the prosecution performance in clear-cut cases. Its effect is, however, very patchy in practice. Numerous victims continue to experience obstacles in reporting incidences such as fear of stigma, ignorance regarding the legal process and lack of confidence on whether their report will be taken seriously. Moreover, cyber evidence is usually technical in nature, making it challenging to investigate and prepare a case, compromising enforcement results.

In spite of these advantages, there are still a number of structural and cultural issues that constrain the full efficiency of the legal framework. Reporting mechanisms are yet to be fully used and in other scenarios, the victims might not use the legal channels because of the social pressure or privacy concerns. There is also a greater institutional capacity need in evidence collection and tracing in digital form to facilitate timely and precise prosecution of offenders. Moreover, the legal framework is sound in theory, but it is not as much integrated in the consciousness of the population and in daily digital practices. With the increased integration of digital communication into everyday life, there is a need to shift toward preventive measures and reduce enforcement through reaction. This involves awareness campaigns, enhanced reporting, and enhanced collaboration between the law and technology. Improving these aspects will assist in ensuring that the legislation is not only effective in punishment but also in preventing and changing behavior in the long term.

FUNDING:

Proposal Number: KFU263581

References

1. Alabdulatif, A. (2018). Cybercrime and analysis of laws in the Kingdom of Saudi Arabia [Master's thesis]. <https://uh-ir.tdl.org/bitstreams/9679624e-9f9e-48cd-bcf6-4524a14df8a3/download>
2. Al-Rahmi, W. M., Yahaya, N., Alamri, M. M., Aljarboa, N. A., Kamin, Y. B., & Moafa, F. A. (2019). A model of factors affecting cyber bullying behaviors among university students. *IEEE Access*, 7, 2978–2985 https://scholar.google.com/citations?view_op=view_citation&hl=en&user=ZcLEuDYAAAAJ&citation_for_view=ZcLEuDYAAAAJ:hqOjcs7Dif8C
3. Alsulami, A. K. (2022). Anti-cybercrime legislation in the Kingdom of Saudi Arabia: A critical analysis [Doctoral thesis, University of Leeds]. <https://etheses.whiterose.ac.uk/id/eprint/30531/1/Alsulami%20thesis%20final%20version%20clean.pdf>
4. Kingdom of Saudi Arabia. (2007). Anti-Cyber Crime Law (Royal Decree No. M/17). [https://www.mcit.gov.sa/sites/default/files/2021-06/la_004_e_anti-cyber_crime_law%20\(1\).pdf](https://www.mcit.gov.sa/sites/default/files/2021-06/la_004_e_anti-cyber_crime_law%20(1).pdf)
5. Kingdom of Saudi Arabia. (2018). Anti-Harassment Law. <https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/f9de1b7f-7526-4c44-b9f3-a9f8015cf5b6/2>
6. Moafa, F. A. (2014). Classifications of cybercrimes-based legislations: A comparative research between the UK and KSA. *International Journal of Advanced Computer Research*, 4(2), 699–705. (Available via Google Scholar profile: <https://scholar.google.com/citations?user=ZcLEuDYAAAAJ&hl=en>)
7. Moafa, F. A., Ahmad, K., Al-Rahmi, W. M., Alias, N., & Obaid, M. A. M. (2018a). Factors for minimizing cyber harassment among university students: Case study in Kingdom of Saudi Arabia (KSA). *Journal of Theoretical & Applied Information Technology*, 96(6). <http://www.jatit.org/volumes/Vol96No6/14Vol96No6.pdf>
8. Moafa, F. A., Ahmad, K., Al-Rahmi, W. M., Yahaya, N., Kamin, Y. B., & Alamri, M. M. (2018b). Cyber harassment prevention through user behavior analysis online in Kingdom of Saudi Arabia (KSA). *Journal of Theoretical & Applied Information Technology*, 96(6). <http://www.jatit.org/volumes/Vol96No6/25Vol96No6.pdf>
9. Moafa, F. A. (2018). Integrated-system to minimizing cyber harassment in kingdom of Saudi Arabia (KSA). *International Journal of Engineering & Technology*, 7(4), 2192–2196. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=ZcLEuDYAAAAJ&citation_for_view=ZcLEuDYAAAAJ:3fE2CSJrl8C
10. Moafa, F. A. (2026). Digital harassment and cyberstalking in the Saudi community: A socio-legal analysis of risk factors, reporting barriers, and preventive strategies. *International Journal of Advances in Signal and Image Sciences*, 327–339. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=ZcLEuDYAAAAJ&citation_for_view=ZcLEuDYAAAAJ:QIV2ME_5wuYC

11. Mukred, M., Mokhtar, U. A., Moafa, F. A., et al. (2024). The roots of digital aggression: Exploring cyber-violence through a systematic literature review. *International Journal of Information Management Data Insights*, 4(2), 100281. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=ZcLEuDYAAAAJ&citation_for_view=ZcLEuDYAAAAJ:ULOm3_A8WrAC
12. UN Women Arab States. (2025). Digital violence in the Arab States: Overview and legal frameworks. <https://arabstates.unwomen.org/sites/default/files/2025-11/final-english-difiviolence-publication.pdf>.