International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(5s) 2026 pp. 410-417
https://doi.org/10.70917/ijcisim-2026-2722
Article

CYBERCRIME LEGISLATION AND THE PROTECTION AGAINST ONLINE RACISM AND CYBERBULLYING: A COMPARATIVE LEGAL ANALYSIS

Hamad Salem Almarri[1], Fahad Abdullah Moafa[2]

[1]Department of Law, College of Law, King Faisal University, Hofuf, Al-Ahsa, Saudi Arabia.
Email: halmarri@kfu.edu.sa
ORCID: 0009-0007-2990-1311
[2]Department of Computer Science, King Fahad Naval Academy, Jubail, Saudi Arabia.
Email: fah171393@hotmail.com
ORCID: 0000-0003-2963-8158

Abstract: The recent exponential increase in the development of digital platforms has increased online racism and cyberbullying, which tend to be inconsistent because they are all types of digital aggression leading to psychological damage, social segregation, and incitement to violence. This comparative legal study explores cybercrime in the Kingdom of Saudi Arabia (KSA), the United Kingdom (UK), and the European Union (EU) through the Digital Services Act (DSA), with a brief US comparison, on safeguarding against online racism (hate speech based on race/ethnicity) and cyberbullying/harassment. The paper is based on the research of Dr. Fahad A. Moafa, such as his comparative typology of cybercrimes in the UK and KSA, models of factors influencing cyberbullying in university students, comparisons of user behavior as a means of prevention. The analysis compares and contrasts definitions of offenses, platform duties, enforcement, and balance with freedom of expression with the help of doctrinal and comparative approaches. The results put emphasis on the criminal sanctioning of KSA in line with Sharia and national security, as compared to the national responsibility of care of the UK and systemic mitigation of risk by the EU. Hybrid models, which combine behavioral prevention and platform accountability, with Arab contexts, are recommended.

Keywords: cybercrime legislation, online racism, cyberbullying, cyber harassment, KSA Anti-Cybercrime Law, UK Online Safety Act, EU Digital Services Act, comparative law, digital aggression.

1. INTRODUCTION

It is now a hallmark of the digital age wherein internet racism and cyberbullying are perpetuated by anonymity, quick content spread, and the permanence of the online environment. These circumstances allow people to use hate speech, either based on race, ethnicity, or national origin, or to be harassed and cyberstalked repeatedly, and the perpetrator might not always be held accountable. Psychological and social impacts are well-established such as anxiety, depression, social withdrawal, and in certain instances, a shift to offline harm (Mukred et al., 2024).

In the Kingdom of Saudi Arabia (KSA) and the wider Arab communities, such harms are influenced by the cultural beliefs that place more emphasis on honor, reputation, and family unity. This kind of norms can make the victims unwilling to report abuse because of the fear of being stigmatized or damaged reputations, which subsequently hides the real magnitude of the issue. Simultaneously, fast digital transformation as part of Vision 2030 has widened access to the internet and social media, providing more opportunities to communicate and exposure to the risks found online.

Legally, KSA is founded on the Anti-Cybercrime Law of 2007, which takes a wide and principle-oriented approach by criminalizing such acts as defamation, invasion of privacy, and violations of public order. Nevertheless, such a framework does not necessarily effectively differentiate between certain types of online harm like cyber bullying. The United Kingdom, in contrast, has come up with more specific legislation, such as the Malicious Communications Act, the Communications Act, and the more recent Online Safety Act 2023, which specifically covers harmful online communication and holds digital platforms to account.

Empirical and socio-legal research also emphasizes that the legal actions are not enough. According to research by Moafa and others, digital literacy, behavioral pattern, social norms, and trust in institutions are key factors that determine the prevalence of cyber harassment, as well as the potential to report it. A significant problem in the Saudi context is cultural barriers especially in terms of honor and privacy.

Internationally, through conventions like the Additional Protocol to the Convention on Cybercrime and the Digital Services Act adopted by the European Union, the current focus on the accountability of platforms, their transparency, and proactive regulation of online harms has become more evident. These developments offer effective guidelines with which to analyze national legal systems.

Regardless of the legal frameworks that exist in KSA, online racism and cyberbullying are underreported and under-addressed. The fact that the current laws are broad in nature, and that the socio-cultural factors prevent reporting on certain cases of digital harm restrict its ability to address particular instances of the harm. Concurrently growing digital interaction has enhanced vulnerability to these dangers, generating a disconnect between the law and actualities.

This study aims to:

a) Research the phenomenon of internet racism and cyberbullying during the digital age and its effects.

b) Examine the usefulness of the Anti-Cybercrime Law of KSA to curb harms on the internet.

c) Compare the legal system in Saudi Arabia and that of the United Kingdom.

d) Discover how behavioral, social, and cultural factors influence cyber harassment.

e) Assess foreign legal systems and their applicability in the Saudi environment.

f) Suggest culturally sensitive and legally viable measures to deal with online harms.

The work adds to the body of existing literature since it incorporates law, behavioral, and social-cultural points of view on the issue of cyberbullying and online racism. It offers a comparative insight of the various strategies of regulation and the significance of culture in policy success. The results are expected to aid in creating more sensitive laws within the Arab communities.

The analysis will revolve around cyberbullying and internet racism in the Saudi Arabian context with comparative inferences made on the United Kingdom and the European Union. It reflects legal analysis, empirical research, international regulatory developments to provide a thorough understanding of the issue.

2. METHODS

Data Sources

The research is based on primary as well as secondary sources to substantiate a comparative legal analysis. The main sources of law are the Anti-Cybercrime Law (2007) of the Kingdom of Saudi Arabia, the Online Safety Act (2023) of the United Kingdom, and the Digital Services Act (2022) of the European Union. These laws form the fundamental foundation of analyzing the manner in which various jurisdictions address racism and cyber bullying over the internet. Besides these laws, the research study is based on secondary sources, such as academic literature, peer-reviewed publications, but mostly the research of Moafa and similar socio-legal investigations. The international legal tools, including the Additional Protocol to the Convention on Cybercrime created by the Council of Europe, are also included as they give a more global picture and help in the comparative application.

Analytical Framework

This study is organized into the comparative framework, which assesses the most important aspects of cybercrime laws in different jurisdictions. Particularly, the paper will look at the manner in which each of the legal systems classifies pertinent crimes, such as online racism, hate speech and cyberbullying. It also evaluates the role and responsibility of digital platforms, especially in regards to the content moderation and risk management.

Machinery of enforcement is discussed to learn the way laws are enforced in practice, such as regulatory control and sanctions. Moreover, the framework also takes into account the level of protection of victims by each system and the availability of remedies. Lastly, the paper assesses the balance between regulating harmful content and the freedom of expression as applied by each jurisdiction which is one of the key legal and ethical issues in digital governance.

Limitations

There are a number of limitations that apply to this study. To begin with, legislation addressing cybercrime is quickly changing, especially in the jurisdiction like the UK and the EU, which can influence the applicability of some of the findings in the long-run. Second, there are differences in the availability and transparency of data across jurisdictions, especially in relation to enforcement practices and reporting rates. The differences may complicate direct comparisons. Even though such limitations may be considered, the research bases itself solely on legal documents and peer-reviewed academic literature that are confirmed, which guarantees the high degree of reliability and academic rigor of the research.

3. RESULTS AND FINDINGS

One of the main insights of the research is that the definition and understanding of online harms (especially online racism and cyberbullying) differ considerably across different jurisdictions. The Kingdom of Saudi Arabia (KSA) has a legal system that is broad and principle-oriented provisions of the Anti-Cybercrime Law (2007). Instead of directly defining cyberbullying or online racism as specific criminal acts, the legislation deals with such phenomena using such general terms as defamation, invasion of privacy, and actions that cause disorder and threat to the order and moral principles in a community (Moafa, 2014). This is an elastic strategy that enables the authorities to use the law to a broad spectrum of online misbehaviors. Nonetheless, it also creates ambiguity because lack of specific definitions can result in differences in interpretation and application.

The United Kingdom on the other hand is more structured and detailed in its approach in the law. The UK also has more specifications on harmful online behaviors through legislation, including the Online Safety Act (2023), which encompasses an abusive communication provision, a harassment provision, and a child protection provision (UK Government, 2023). Such specificity increases the clarity of the law and its enforcement by making sure that various types of harm on the Internet are clearly defined. The Digital Services Act (2022) of the European Union uses a different strategy as it does not prioritize the definition of particular crimes but rather highlights systemic risks of harmful content. According to the DSA, the platforms are to detect and reduce risks like hate speech and harassment (European Union, 2022).

The differences represent three regulatory philosophies, a general and liberal approach in KSA, a categorized and specific system in the UK and a systemic and preventive approach in the EU (Brown, 2018; Waldron, 2012).

In Saudi Arabia, the practice is mainly state-based, and the government has the role of detecting and criminizing cyber crimes. Platforms are not main regulators but supportive (Moafa, 2014). This is indicative of a classical legal paradigm where the state continues to have the control of enforcement. In the United Kingdom both the state and the private platforms share the responsibility. The Online Safety Act (2023) establishes a duty of care that obliges platforms to proactively prevent harmful content to users, and regulating it is done by Ofcom (UK Government, 2023). This is a move towards collective responsibility.

European Union goes a step higher to put platforms at the heart of regulation. Digital services Act requires very large online platforms to perform risk assessment, maintain transparency, and take mitigation measures to decrease harmful content (European Union, 2022). The methodology can be compared to the general tendencies in digital governance where platforms are viewed as major actors that contribute to online safety (Gillespie, 2018).

In general, these strategies indicate a shift in the world towards reactive enforcement to active governance (OECD, 2021).

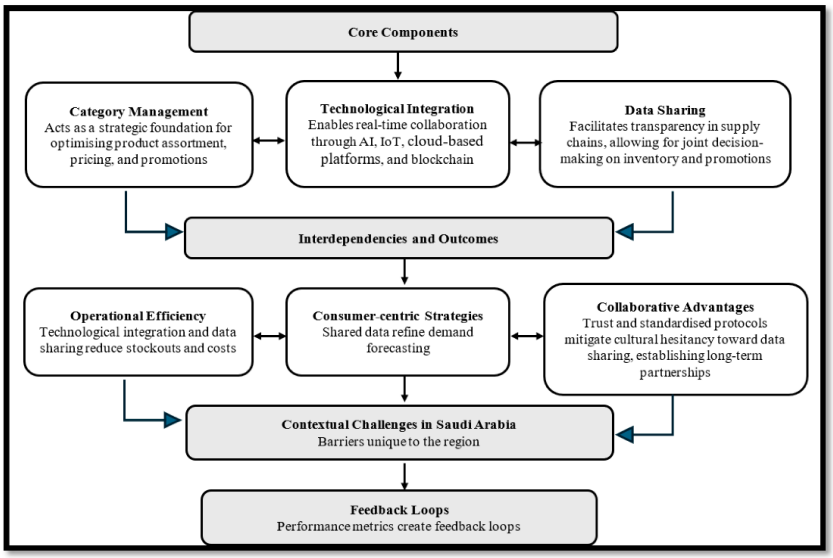

Figure 1:The Efficacy of Technological Integration and Data Sharing

In addition to legal systems, cultural and behavioral aspects are also crucial in defining cyber bullying and online racism. The empirical studies reveal that social norms, perceived anonymity, and the awareness of legal regulations affect online harmful behavior (Al-Rahmi et al., 2019; Hinduja and Patchin, 2015). These are some of the factors that lead to normalization of aggressive online communication.

The Saudi culture, as it is applicable to honor, reputation and family cohesion, has a tremendous influence on reporting behavior. Underreporting and ineffectiveness of the law may also be caused by fear of stigma or social repercussions that compel victims not to report incidents (Moafa et al., 2018a; Mukred et al., 2024). This makes a discrepancy between legal provisions and actual performances.

These results imply that educational programs, awareness campaigns, and culturally competent reporting systems should be used to complement legal solutions to effectively resolve online harms (Citron, 2014).

Figure 2: Theoretical structure of relations among cultural factors

Cyberbullying has its dynamics which can be comprehended in terms of a behavioral model. Personal attitudes, social pressure, and perceived anonymity are some of the inputs that expose one to the risks of engaging in harmful online behavior. They cause such behaviors as cyberbullying and online racism that lead to psychological damage,

social isolation, and underreporting (Al-Rahmi et al., 2019; Mukred et al., 2024). This cycle perpetuates itself, with a lack of reporting decreasing accountability and letting harmful behavior continue.

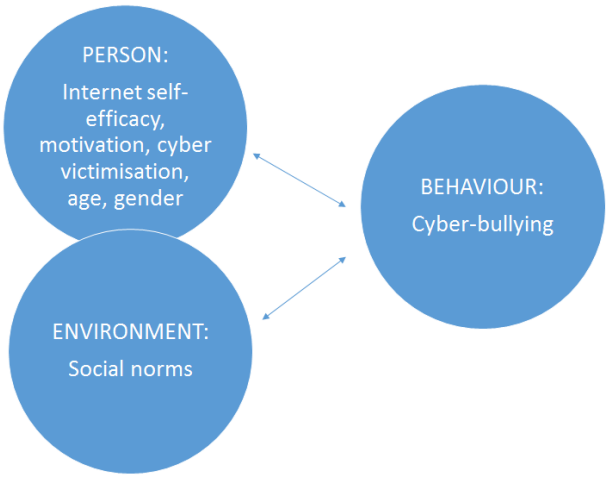

Figure 3: Motivators to Cyberbullying Behaviour.

One similarity that can be observed in all jurisdictions is the fact that the implementation of cybercrime laws in a digital world is a challenge. Online platforms are borderless and dangerous propaganda is usually created beyond national jurisdictions. This poses a big challenge in terms of enforcement.

The jurisdictional constraints do not allow the authorities to effectively prosecute offenders who are situated in other countries and the dissimilarity in the legal norms makes cooperation in the international system hard (Council of Europe, 2003). Also, most of these platforms are based in other countries, and local regulation is restricted.

These issues show that there should be greater international collaboration and coordinated legal systems. The existence of enforcement gaps will not disappear even with powerful domestic legislations without concerted actions (OECD, 2021).

The relative comparison indicates unique strengths and weaknesses within jurisdictions. The Saudi Arabian strategy offers powerful criminal penalties and integrates socio-cultural factors, but is not specific and does not include proactive mechanisms (Moafa, 2014). The frameworks in the UK and the EU focus on prevention via accountability of platforms, allowing faster responses to harmful content, but issues of overregulation and freedom of expression are also of concern (Gillespie, 2018; Waldron, 2012).

An opposite case is the United States, which values the freedom of speech and grants immunity to platforms to a wide extent under Section 230, thus offering less protection against harm online (Citron, 2014). Although this would protect the freedom of the individuals, it would have major loopholes in protecting the victims.

4. DISCUSSION

The comparative analysis shows that there is a significant gap between the formal power of the legal frameworks and their practical usefulness in combating the online racism and cyberbullying. The Anti-Cybercrime Law (2007) in the Kingdom of Saudi Arabia (KSA) offers a solid legal framework with extensive criminal offenses to cover defamation, privacy invasion, and other harmful Internet behavior. They are broad enough to encompass all types of behavior, such as cyberbullying and online racism, despite the fact that they are not clearly characterized as distinct crimes (Moafa, 2014). Such flexibility however comes at a price. This lack of clear legal definitions gives rise to ambiguity, which may result in unequal application and confusion of the victims and the authorities on what is punishable behavior.

In addition to legal ambiguity, culture is also a major contributor to real-life implications of these laws. The culture of honor, reputation and social cohesion, which is highly valued in Saudi society, may prevent victims of online forms of abuse to report. They might be afraid of social stigma, reputation destruction, or family consequences, especially when it comes to harassment or humiliation in front of the crowd (Moafa et al., 2018a; Mukred et al., 2024). This means that a lot of cases are never reported and this undermines the deterrent power of the law and reduces its

practicality. Also, the comparatively small scope of digital platforms in content regulation in the Saudi context, implies that dangerous content can be left on the internet longer, potentially affecting victims more.

Conversely, the EU and the United Kingdom have followed a more proactive regulation strategy based more on prevention than just punishment. The Online Safety Act (2023) of the UK provides a duty of care which obliges the platforms to actively reduce harmful content, whereas the Digital Services Act (2022) of the EU offers a risk assessment and mitigation of the large platforms (European Union, 2022; UK Government, 2023). The frameworks tend to be more efficient in dealing with harm earlier in the process, limiting the dissemination and effects of harmful content. Nonetheless, they are not unscathed. Researchers and policy makers have expressed reservations that heightened platform accountability can result in over-regulation and excessive content deletions and that it can cause a violation of freedom of expression (Gillespie, 2018; Waldron, 2012). The use of automated moderation systems also brings in the risks of bias and over-censorship.

This analogy reveals one of the inherent contradictions in regulation of cybercrime; the necessity to provide effective protection against harm with the maintenance of individual freedoms. Although KSA approaches are more focused on social order and cultural values, UK and EU systems are more focused on user protection, which is achieved by systemic regulation at the cost of the issue of free speech. In neither case is this tension completely resolved.

The results of this research are a great indication of why a hybrid regulatory model that incorporates the merits of the various legal systems should be adopted with the shortcomings of the various systems being addressed. A single jurisdiction exists that is yet to offer a holistic approach to the situation of online racism and cyberbullying. Rather, it is essential to have a powerful framework that integrates the aspects of criminal law enforcement, platform responsibility, and behavioral intervention.

To begin with, tough criminal enforcement measures, which are a feature of KSA, are still necessary. Laws are a preventative measure and offer a formal system to deal with extreme instances of cyber bullying. Nevertheless, these legislations need to be updated to incorporate more detailed definitions of cyberbullying and online racism to minimize uncertainty and enhance consistency in enforcing the law (Brown, 2018).

Second, the proactive involvement of digital platforms, which the UK and EU models focus on, is essential in averting harm before it takes off. It is platforms that are strategically placed to monitor users and detect dangerous content and take action promptly. Platforms should then be mandated by regulatory frameworks to have transparent moderation measures, regularly evaluate risks, and be accountable to their actions (OECD, 2021).

Third, any effective response needs to include behavioral prevention strategies. Studies indicate that social norms, attitudes, and anonymity impact cyberbullying (Al-Rahmi et al., 2019; Hinduja and Patchin, 2015). These factors can be redefined through educational programs, digital literacy programs, and public awareness programs, which will minimize the chances of engaging in harmful behavior. In culturally sensitive environments like Saudi Arabia, such interventions must be specific to the social values and deal with barriers to reporting.

A combination of these three elements will result in a hybrid model that should deal with the causes and effects of online harm. It goes beyond a purely reactive or purely preventive solution, providing a more balanced and comprehensive solution.

The hybrid model proposed can be conceptualized as three-layered system. The first level is legal enforcement in which the criminal law forms the basis in the consequences of serious crimes and accountability. The second layer involves platform responsibility where digital service providers are expected to actively screen, evaluate, and control the risk posed on malicious content. The third layer focuses on the prevention of behavior, which incorporates education, awareness, and cultural aspects to lessen the chances of the harmful behavior occurring in the first place. These layers are combined to constitute an overall protection system that is functional in legal, technological, and social scales.

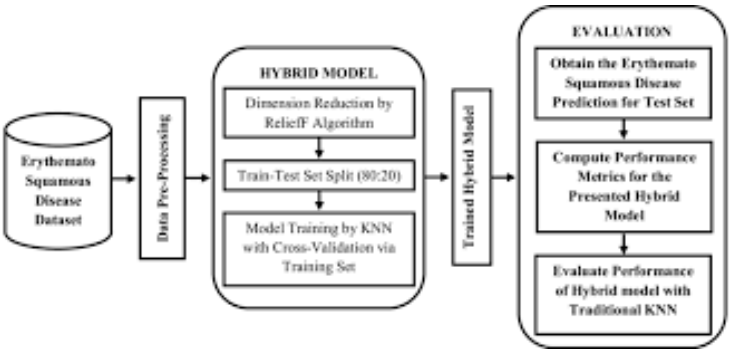

Figure 4: Hybrid Regulatory Framework.

There are a number of implications of the move towards a hybrid regulatory model on policymakers. First, there is need to enhance legal definitions of cyberbullying and online racism especially in jurisdictions where the current laws are based on broad categories. Clarity in definitions leads to increased legal certainty, better enforcement and assurance of the understanding of their rights by the victims.

Second, policymakers need to focus on creating convenient and culturally responsive reporting systems. Anonymous reporting mechanisms and support services can be utilized in situations where victims are not encouraged to report because of social stigma, which results in more victims being included and enhancing the data collection process. This, consequently, enhances the general efficiency of legal systems.

Third, the responsibility of platforms should also be enhanced by regulatory interventions that would entail transparency, risk evaluation, and monitoring of compliance. To make sure that the processes of content moderation are effective and do not violate the basic rights, governments should collaborate with technology companies.

Lastly, international collaboration is needed. With the cross-border nature of digital platforms, it is not possible to effectively counter online harms in a single country. The jurisdictional gaps should be bridged by collaboration frameworks, common standards and coordinated enforcement efforts to provide uniform protection across the borders (Council of Europe, 2003; OECD, 2021).

5. CONCLUSION

Based on the comprehensive research of Moafa on cyber harassment, cyberbullying and comparative legal systems, this analysis illustrates that KSA offers culturally sensitive criminal law instruments, which resonate with the values of the society like public order and reputation protection. These laws are also versatile and able to respond to a broad spectrum of online harms, however they work best when they are reinforced by proactive, behaviour-based initiatives. Conversely, the Digital Services Act of the European Union and the Online Safety Act 2023 of the United Kingdom focus on the accountability of the platforms, with digital services having the responsibility of proactively detecting and removing harmful content. This passes the burden off of individual criminals to systematic control. An equal, hybrid strategy that combines the legal capabilities of KSA with proactive platform regulation and education-based interventions provide the best way ahead, which would protect against online racism and cyberbullying and yet acknowledge freedom of expression.

RECOMMENDATIONS

1) Revise KSA provisions to have clear intersections of racism and harassment as the socio-legal understanding of Moafa.
2) Embrace hybrid models: DSA-like risk assessment and Moafa-et-al. behavioral prevention models.
3) Enhance reporting to overcome cultural barriers reported in Saudi studies.
4) Enhance GCC/Arab collaboration in cross-border cases, in the footsteps of Moafa.
5) Invest in Sharia-compliant digital tools to investigate.
6) Promote culturally sensitive moderation of platforms.
7) Fund additional studies on the basis of the digital aggression and harassment studies of Moafa.

FUNDING:

Proposal Number: KFU263580

References

1. Al-Rahmi, W. M., Yahaya, N., Alamri, M. M., Aljarboa, N. A., Kamin, Y. B., & Moafa, F. A. (2019). A model of factors affecting cyberbullying behaviors among university students. IEEE Access, 7, 2978–2985. https://doi.org/10.1109/ACCESS.2018.2886560
2. Anderson, M. (2018). A majority of teens have experienced some form of cyberbullying. Pew Research Center. https://www.pewresearch.org
3. Brown, A. (2018). What is hate speech? Part 1: The myth of hate. Law and Philosophy, 37(4), 419–468. https://philpapers.org/rec/BROWIH
4. Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press. https://digitalcommons.law.umaryland.edu/books/91/
5. Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. https://www.coe.int/en/web/cybercrime/first-additional-protocol
6. European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). https://eur-lex.europa.eu/eli/reg/2022/2065/oj
7. Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press. https://www.scirp.org/reference/referencespapers?referenceid=2935670
8. Hinduja, S., & Patchin, J. W. (2015). Bullying beyond the schoolyard: Preventing and responding to cyberbullying (2nd ed.). Sage Publications. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-r038/2015-r038-eng.pdf
9. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review. Psychological Bulletin, 140(4), 1073–1137. https://doi.org/10.1037/a0035618
10. Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. Journal of Child Psychology and Psychiatry, 55(6), 635–654. https://doi.org/10.1111/jcpp.12197
11. Moafa, F. A. (2014). Classifications of cybercrime-based legislations: A comparative research between the UK and KSA. International Journal of Advanced Computer Research, 4(2), 699–705.
12. 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 and Applied Information Technology, 96(6), 1530–1543.
13. 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 KSA. Journal of Theoretical and Applied Information Technology, 96(6), 1544–1555.
14. Mukred, M., Mokhtar, U. A., Moafa, F. A., Gumaei, A., Sadiq, A. S., & Al-Othmani, A. (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://www.sciencedirect.com/science/article/pii/S2667096824000703
15. OECD. (2021). Regulating digital platforms: A global perspective. Organisation for Economic Co-operation and Development. https://www.oecd.org
16. Pew Research Center. (2022). Teens and cyberbullying 2022. https://www.pewresearch.org
17. Perry, B., & Olsson, P. (2009). Cyberhate: The globalization of hate. Information & Communications Technology Law, 18(2), 185–199. https://doi.org/10.1080/13600830902814984
18. Patchin, J. W., & Hinduja, S. (2018). Sextortion among adolescents. Sexual Abuse, 30(5), 541–561. https://pubmed.ncbi.nlm.nih.gov/30264657/
19. United Kingdom. (2023). Online Safety Act 2023. https://www.legislation.gov.uk/ukpga/2023/50
20. United Nations Human Rights Council. (2021). The promotion, protection and enjoyment of human rights on the Internet. https://www.ohchr.org
21. U.S. Congress. (1996). Communications Decency Act, Section 230. https://www.law.cornell.edu
22. Waldron, J. (2012). The harm in hate speech. Harvard University Press. https://psycnet.apa.org/record/2012-13213-000
23. Williams, M. L., Burnap, P., & Sloan, L. (2017). Crime sensing with big data. British Journal of Criminology, 57(2), 320–340. https://doi.org/10.1093/bjc/azw042