SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 2508-2517
Open Access. Online & Print

DOI: 10.5281/zenodo. 18848558

THE CRIMINAL LAW RESPONSE TO CYBERBULLYING: A COMPARATIVE ANALYSIS OF OMANI, US, UK, AND FRENCH LEGISLATION

Ahmad Mohamad Alomar[1], Abdullah Ali Salim Al. Shibli[2], Said Ali Hassan Al. Mamari[3], Radwan Ahmad Al-Haf [4], Zaki Mohamed Channak[5]

[1]AAlomar@su.edu.om. ORCID No: https://orcid.org/0009-0006-8000-9700
Assistant Professor, Faculty of Law, Sohar University. Sohar, Oman
[2]AASShibli@su.edu.om. ORCID No: https://orcid.org/0000-0001-8662-4225
Associate Professor, Faculty of Law, Sohar University. Sohar, Oman
[3]SAMamari@su.edu.om. ORCID No https://orcid.org/0009-0002-7989-4985
Associate Professor, Faculty of Law, Sohar University. Sohar, Oman
[4]RAlHaf@su.edu.om. ORCID No https://orcid.org/0009-0007-9469-657X
Assistant Professor, Faculty of Law, Sohar University, Sohar, Oman
[5]zchannak@psu.edu.sa ORCID No https://orcid.org/0009-0009-7872-4678
Associate Professor, Faculty of Law, Sultan Prince University, KSA

Received: 20/10/2025
Accepted: 01/12/2025

Corresponding Author: Ahmad Mohamad Alomar (AAlomar@su.edu.om)

ABSTRACT

This paper examines cyberbullying as a distinct form of digitally mediated harm that challenges traditional categories of criminal law. Using a comparative doctrinal and case-law analysis of the Omani, American, British, and French legal systems, it evaluates whether existing penal and cybercrime frameworks can genuinely accommodate the specific features of cyberbullying and provide effective protection for victims. The study argues that cyberbullying is defined by a particular constellation of characteristics—deliberate targeting, repetition or persistence, technological amplification, and structural power asymmetry—that qualitatively distinguish it from related offences such as defamation, threats, privacy violations, and unlawful access to information systems. Drawing on key decisions of the United States Supreme Court on online threats and harassment, as well as leading judgments of the European Court of Human Rights and recent rulings of the Omani Supreme Court on insult and violations of private and family life committed via digital means, the paper shows both the flexibility and the limits of applying existing offences to sustained online abuse under robust free-speech guarantees. The comparative findings reveal a fragmented regulatory landscape. French law has moved towards explicit criminalisation of cyberbullying, many U.S. states have adopted specialised anti-bullying statutes within tight constitutional constraints, and the United Kingdom relies on a dispersed set of communications and harassment offences. By contrast, Omani law still addresses cyberbullying only indirectly through general penal and cybercrime provisions, leaving significant gaps regarding behaviours such as impersonation, systematic exclusion, and coordinated digital attacks. In light of these results, the paper proposes a tailored legislative framework for Oman that recognises cyberbullying as an autonomous criminal offence and complements criminal sanctions with preventive, educational, and technical measures, seeking to reconcile robust protection of psychological integrity and human dignity with constitutional guarantees of freedom of expression.

KEYWORDS: Cyberbullying, Comparative Criminal Law, Digital Harassment, Online Safety, Judicial Interpretation, Legislative Reform.

1. INTRODUCTION

This introduction outlines the escalating phenomenon of cyberbullying, presents comparative legislative responses, and frames the core research problem regarding the necessity and form of its criminalisation.

The proliferation of digital communication technologies and the pervasive use of social media platforms have generated new forms of harmful and antisocial conduct collectively referred to as cyberbullying. The term denotes a pattern of repeated and intentional behaviour perpetrated through electronic communication tools or online networks with the aim of inflicting psychological or emotional harm upon the victim (Alomar & Alabady, 2023). This phenomenon increasingly affects wide segments of society, particularly adolescents and students, who constitute the most frequent users of digital platforms. Recent scholarship reports that nearly 95% of teenagers in the United States have access to smartphones, a factor strongly correlated with rising cyberbullying rates (Hallmark, 2023). Victims of cyberbullying are almost twice as likely to attempt suicide (Abdelaziz, 2025a) compared to their non-victimized counterparts (Hallmark, 2023).

Similarly, research conducted in the United Kingdom indicates that approximately half of 35,000 surveyed students reported exposure to some form of online harassment, while nearly 30% experienced cyberbullying at some point in their lives (Ditch the Label, 2013). Global surveys also show that seven out of ten internet users have faced online abuse (Al-Harbi, 2019). In Oman, official statistics issued by the Public Prosecution on 16 February 2023 reveal a steady rise in online insult and defamation cases between 2018 and 2022—from 481 cases in 2018 to 1468 cases in 2021, before slightly decreasing to 1328 cases in 2022.

From a comparative legal perspective, there is no federal statute in the United States that explicitly criminalises conduct under the specific label of "cyberbullying" (Al-Najjar, 2022). However, forty-nine out of fifty states have enacted legislation addressing various forms of cyberbullying, albeit with considerable variation in definitions, scope, and penalties (Al-Najjar, 2022). For example, California's Penal Code § 653.2 specifically addresses electronic harassment, while New York's Education Law § 12-d focuses on cyberbullying in schools, illustrating the diverse state-level approaches. Several jurisdictions—such as France, Egypt, and Greece—have amended their penal codes to incorporate provisions targeting harmful online behaviour. France, in particular, expanded Article 222-33 of its Penal Code by virtue of Law No. 2014-873 of 4 August 2014, thereby criminalising multiple forms of bullying and providing aggravated penalties when committed through digital means (LOI n° 2014-873 du 4 août 2014, art. 40). In practice, French courts have applied these provisions to cases of sustained digital harassment, reinforcing the link between legislative text and judicial enforcement. French law also addresses cyberbullying manifestations through hate-speech legislation and offences relating to online harassment.

In contrast, the Omani legal system contains no express statutory provisions dedicated to cyberbullying as a distinct offence. This legislative lacuna raises an essential inquiry: Are the existing provisions of the Omani Penal Code and the Cybercrime Law adequate to encompass the multifaceted manifestations of cyberbullying, or is the enactment of specialised legislation necessary?

The significance of the present study lies in the growing severity and complexity of cyberbullying, particularly considering the anonymity, speed, and expansive reach of digital platforms, and the limited regulatory oversight over social media networks. Given that cyberbullying remains relatively underexamined in Arab jurisdictions, this research contributes to one of the earliest and most comprehensive legal analyses of the issue within the region. Its findings also bear practical importance for guiding national legislators in reforming penal and cybercrime statutes—or adopting dedicated laws—to confront cyberbullying effectively and reduce its prevalence.

The core research problem concerns whether cyberbullying acts should be regarded as criminal offences and whether their criminalisation requires new legislative provisions. This problem raises several subsidiary questions: Does criminalising cyberbullying conflict with the right to freedom of expression? To what extent is specialised legislation necessary to ensure effective legal protection against cyberbullying?

This study adopts a comparative analytical methodology, examining relevant provisions in Omani, US, UK, and French law to assess their applicability to various forms of cyberbullying and determine the extent to which existing legal frameworks address or fail to address these behaviours.

A number of academic studies have explored cyberbullying from different legal perspectives. El-Toni highlights the persistent ambiguity surrounding the legal definition of electronic bullying and its intersection with related offences,

emphasising the insufficient reach of existing criminal provisions (Al-Toni, 2016). Al-Khasawneh concludes that most forms of cyberbullying fall within the remit of Jordan's Cybercrime Law, although gaps remain (Al-Khasawneh, 2020). Al-Lam'i underscores the deliberate and repetitive nature of cyberbullying and stresses the need for precise legislative responses (Al-Lam'i, 2021). These studies collectively demonstrate the fragmented state of legal scholarship and the need for deeper comparative assessment.

To address the problem in a coherent structure, this article proceeds in two substantive sections. The first establishes the necessity of criminalising cyberbullying within modern penal policy. The second articulates its distinctive legal nature and differentiates it from analogous offences, including insult and defamation, invasion of privacy, harassment, and hate-speech offences. The study concludes with key findings and practical recommendations for legislative reform.

2. SECTION I—THE IMPERATIVE OF CRIMINALISING CYBERBULLYING

This section establishes the normative justification for criminalising cyberbullying, addressing central objections grounded in freedom of expression and demonstrating why such criminalisation is a necessary legal evolution to protect psychological integrity and human dignity in the digital age.

Cyberbullying has emerged as an incontrovertible social reality, both pervasive and pernicious in its impact. It constitutes a particularly harmful form of technology-facilitated misconduct that violates human dignity, corrodes self-esteem, and inflicts profound psychological and reputational harm. In response, numerous jurisdictions have enacted dedicated statutory provisions or amended existing penal and cybercrime frameworks to address its multifarious manifestations. This development prompts a central jurisprudential inquiry: is it necessary to recognise cyberbullying as a distinct criminal offence?

A recurrent objection asserts that criminalising cyberbullying represents an undue encroachment upon freedom of expression. It is argued that the imposition of criminal sanctions on online speech—particularly where such speech takes the form of criticism, commentary, or dissent—undermines democratic discourse and may conflict with constitutional guarantees such as the First Amendment to the United States Constitution (Cornell Law School, 2022). This perspective, however, neglects the specific and substantial harms intrinsic to cyberbullying. The conduct systematically erodes the victim's psychological integrity, disrupts social cohesion, and fosters discrimination, hostility, and social fragmentation. It thereby undermines fundamental legal interests, including equality, peaceful coexistence, and the protection of personal dignity in its moral and emotional dimensions (Channak, 2026).

Freedom of expression undoubtedly constitutes a cornerstone of democratic societies. It is firmly embedded in international human rights instruments such as Article 19(2) of the International Covenant on Civil and Political Rights and the 1948 Universal Declaration of Human Rights, and similarly protected in domestic constitutional frameworks, including Article 35 of the Omani Basic Law (Royal Decree No 6/2021, art 35). Yet, notwithstanding its foundational status, freedom of expression is not absolute. Comparative jurisprudence consistently demonstrates that it may be subject to reasonable, necessary, and proportionate restrictions designed to safeguard other compelling public interests—such as the protection of mental integrity and the prevention of psychological harm. This judicial principle is affirmed in Board of Education v Pico, where the United States Supreme Court upheld limitations imposed to protect educational integrity and the rights of students to receive appropriate information (Board of Education v Pico, 457 US 853, 867, 1982).

In a similar vein, the United Kingdom's Online Safety Act 2023, Part 3, exemplifies a contemporary legislative model that seeks to reconcile expressive freedom with the regulatory duty imposed on digital platforms to prevent the dissemination of illegal and harmful content, including hate speech, sexual exploitation, coercive control, and content that promotes bullying. This approach recognises that unrestrained expression may lead to violations of public order and personal dignity, thereby justifying statutory intervention.

The exercise of free expression ceases to enjoy legal protection when it degenerates into humiliation, degradation, or psychological abuse. Cyberbullying, by its very nature, crosses this threshold. Judicial authorities have long recognised limits to protected expression. In a seminal judgment issued on 27 February 1932, the Egyptian Court of Cassation held that speech loses its legitimacy when it relies on exaggeration, intimidation, or inflammatory language solely to provoke emotional distress or manipulate belief. Likewise, in Bethel School District v Fraser, the United States Supreme Court upheld disciplinary measures restricting vulgar and offensive speech, recognising that such

expression possesses minimal social value and may legitimately be curtailed to protect vulnerable audiences and safeguard public morality (Bethel School District v Fraser, 478 US 675, 685–86, 1986).

Cyberbullying is distinguished by its persistence, its deliberate infliction of humiliation, and the often-public nature of the harm it causes. The digital medium amplifies the scale and permanence of this harm, granting abusive content instantaneous dissemination and enduring visibility. These distinctive attributes necessitate targeted legislative intervention to recalibrate the balance between expressive freedom and the fundamental rights to dignity, psychological security, and equal participation in digital society. Accordingly, the targeted criminalisation of cyberbullying transcends mere policy discretion; it represents a necessary legal evolution to uphold fundamental rights and preserve social cohesion in an increasingly digitalised world.

3. SECTION II—THE DISTINCTIVE NATURE OF CYBERBULLYING AND ITS DIFFERENTIATION FROM RELATED OFFENCES

3.1. Sub-section I—The Specific Legal Characteristics of Cyberbullying

This sub-section argues that cyberbullying possesses distinctive constitutive attributes and protects a unique legal interest—psychological integrity and digital dignity—which collectively justify its recognition as a sui generis offence rather than its assimilation into traditional criminal categories.

Building upon the established normative justification for criminalising cyberbullying, this section addresses a consequential jurisprudential question: Does cyberbullying's unique legal character necessitate sui generis legislative treatment, or can existing criminal frameworks adequately accommodate its diverse manifestations?

Cyberbullying appears in numerous behavioural forms, including flaming, harassment, stalking, defamation, reputational harm, account intrusion, dissemination of rumours, disclosure of private information, impersonation, exclusion, deception, and various other technology-mediated aggressions. At first glance, these behaviours resemble conventional offences recognised in multiple legal systems, such as insult and defamation, invasion of privacy, unauthorised access to information systems, threats, discriminatory acts, and the misuse of digital networks. The Omani Penal Code, for instance, encompasses insult and defamation under Articles 324–334, while the Cybercrime Law criminalises unauthorised access (Arts 3–10), harmful content (Arts 13–15), and threats (Art 18). Similar parallels may be drawn with US federal law, particularly 18 U.S.C. § 875, which criminalises threatening electronic communications (United States Code, 2024). For example, this statute has been applied in cases involving interstate threats sent via social media, illustrating its use against one form of online aggression.[1]

The central inquiry thus emerges: Can existing punitive provisions be doctrinally adapted to absorb cyberbullying behaviours, or does cyberbullying constitute a distinct legal category requiring bespoke legislative recognition?

A prominent doctrinal view maintains that the absence of specialised statutory provisions does not shield cyberbullies from liability, given the perceived capacity of existing offences to encompass most cyberbullying behaviours. On this account, cyberbullying intersects with established criminal categories that already protect core legal interests, such as reputation, privacy, emotional tranquillity, and data integrity (Ben Rouqia, 2023; Al-Ghafri, 2022). Scholars including Ben Rouqia, Al-Ghāfrī, and Nur al-Hudā argue that cyberbullying is largely subsumable within existing criminal prohibitions, particularly in domains relating to insult, defamation, threats, discrimination, and violations of informational privacy (Ben Rouqia, 2023; Al-Ghafri, 2022).

This assimilationist approach, however, proves normatively and doctrinally insufficient for two principal reasons.

1. Cyberbullying Possesses Distinctive Constitutive Attributes Not Captured by Traditional Offences
While certain cyberbullying acts may coincide with the elements of established crimes, such assimilation denies cyberbullying any autonomous legal identity. It collapses a multifaceted and technologically mediated phenomenon into pre-existing legal categories that fail to capture its unique structure and social harm.

The distinctive legal attributes of cyberbullying include

- Technological Violence—the weaponisation of digital tools, platforms, and networks to inflict harm.

[1] See, e.g., *United States v. Bowker*, 372 F. Supp. 3d 884 (D. Minn. 2019), where the defendant was convicted under 18 U.S.C. § 875(c) for transmitting interstate threats via Facebook, demonstrating the application of this federal statute to threats made through social media platforms.

- Structural Power Imbalance—arising from superior technical skill, anonymity, or the capacity to mobilise large online audiences.
- Systemic Repetition—the persistent or continuously accessible nature of digital content, which produces ongoing harm even without repeated acts by the perpetrator.
- Specific Intent—the deliberate targeting of the victim for humiliation, intimidation, reputational damage, or psychological harm.
- Amplified Harm—the extensive, rapid, and potentially permanent dissemination of abusive content through networked digital environments.

Although these attributes may intersect with traditional offences, they form a composite harm architecture that is greater than the sum of its parts. Many forms of cyberbullying—including impersonation, targeted exclusion, and persistent unwanted contact—fall outside the scope of existing provisions altogether, as illustrated by the Egyptian Cybercrime Law's treatment of "unwanted digital annoyance" under Article 25 (Law No 175 of 2018 on Combating Information Technology Crimes, Egypt), which itself demonstrates the legislative need for specific regulation.

2. Cyberbullying Protects a Distinct Legal Interest: Psychological Integrity and Digital Dignity The assimilationist position also conflates the protected legal interests underlying cyberbullying with those of related offences. Criminalisation is grounded in the protection of specific social interests—each offence safeguarding a particular dimension of public or private welfare (Channak, 2026; Karash, 2022). Thus, insult and defamation protect reputation; privacy offences protect confidentiality; threat offences protect personal safety.

Cyberbullying jurisprudence, however, protects a fundamentally different interest: the individual's psychological integrity and right to digital dignity against systematic, technologically amplified abuse.

Because the protected interest differs substantively from those underlying related offences, cyberbullying cannot be doctrinally reduced to insult, defamation, or privacy violations. Consequently, many modern legal systems have moved toward recognising cyberbullying as an independent criminal offence, justified by the need to protect the emotional and moral inviolability of the human person from sustained digital aggression.

The foregoing analysis demonstrates that cyberbullying possesses a unique legal identity that cannot be fully assimilated within existing offences. Having established its autonomous character, it becomes imperative to systematically differentiate cyberbullying from kindred offences—a task undertaken in the following sub-section through comparative analysis of legal elements, protected interests, and statutory frameworks across jurisdictions.

3.2. Sub-Section II—Distinguishing Cyberbullying from Related Criminal Offences

This sub-section examines the key distinctions between cyberbullying and related offences such as defamation and insult, focusing on differences in *actus reus*, *mens rea*, and protected legal interests across Omani, US, UK, and French legal systems.

Cyberbullying, as established previously, comprises specific constitutive elements that collectively endow it with a distinct legal identity. These defining characteristics set it apart from various forms of aggressive conduct that constitute other closely related criminal offences. This section examines the principal points of differentiation between cyberbullying and key adjacent offences under Omani, US, UK, and French law.

1. Cyberbullying and the Offences of Defamation and Insult Defamation and insult are among the offences most closely related to cyberbullying, as many cyberbullying behaviours manifest as derogatory expressions intended to humiliate the victim, diminish their social standing, or damage their reputation. For instance, the Omani Supreme Court, in Criminal Appeal No. 661/2016 (7 February 2017), upheld a conviction for insult and defamation via information technology tools after the accused posted tweets describing the victims with expressions such as "stupidity," "shameful behaviour," and "their ugly nightly acts"—statements deemed defamatory under Omani law.

Notwithstanding these overlaps, defamation and insult differ from cyberbullying in several key respects.

First, the *actus reus* of defamation and insult consists of communicative conduct—spoken, written, or visual—whereby the perpetrator expresses an opinion or attributes a specific fact capable of harming the victim's honour or reputation. Under Article 326 of the Omani Penal Code, defamation requires attributing a specific fact that would expose the person to punishment or contempt, while Article 327 criminalises expressions violating honour or dignity. French jurisprudence similarly requires, for *diffamation*, the attribution of a sufficiently specific factual allegation injurious to reputation, as confirmed by the Cour de cassation (Criminal Chamber) on 12 April 2005.

By contrast, cyberbullying is characterised not merely by offensive expression but by the perpetrator's exercise of dominance to intimidate, isolate, exclude, or emotionally harm the victim. The communicative act is a medium, not the core harm.

Second, the *mens rea* for defamation and insult is general intent: awareness of the nature of the expressions and intent to convey them (Al-Humaydi, 2021). No specific intent to cause emotional suffering is required. Cyberbullying, however, presupposes specific intent—the deliberate aim of inflicting psychological harm through repeated intimidation, humiliation, or exclusion (Hassan, 2022). In U.S. jurisprudence, this distinction is illustrated in cases like *People v. Marquan M.*, where the court emphasized that cyberbullying involves a deliberate "course of conduct" intended to cause emotional harm, contrasting with the general intent requirement for defamation.[2]

Third, the protected legal interest differs fundamentally. Defamation and insult safeguard honour, reputation, and social standing (Ben Hawwa, 2020). Cyberbullying protects psychological integrity, emotional well-being, and mental security—interests extending beyond reputational harm, justifying a distinct legal response (Al-Tayyar, 2022). This distinction led the French legislature to treat cyberbullying under the framework of *harcèlement moral*.

2. Cyberbullying and Violations of Privacy and Family Life In the United Kingdom, defamation is primarily a civil wrong under the Defamation Act 2013, yet criminal statutes such as the Malicious Communications Act 1988 and the Communications Act 2003 criminalise sending indecent, grossly offensive, or distressing electronic messages with intent to cause harm. The Online Safety Act 2023 amended section 66 of the Sexual Offences Act 2003 to create the offence of "cyber-flashing," including sending genital images or threatening to share intimate images to alarm or humiliate. The first conviction under this provision occurred in March 2024 (BBC News, 20 March 2024). This practical application underscores the UK's approach to criminalising specific, intrusive digital behaviours that overlap with cyberbullying tactics.[3]

In the United States, no federal statute criminalises privacy invasions per se, and most defamation is addressed civilly due to First Amendment constraints. The Supreme Court in *United States v. Alvarez* confirmed that even false statements may enjoy protection absent intent to defraud (*United States v. Alvarez*, 567 U.S. 709, 2012). However, several states criminalise harmful online privacy violations. Florida law penalises electronic dissemination of identifying information with intent to induce reasonable fear (Florida Statutes § 784.048(5)), and Montana's Penal Code (§ 45-8-212) criminalises defamatory electronic communications (Montana Code Annotated § 45-8-212).

French law, under Article 226-1 of the Penal Code, criminalises intentional recording, transmission, or publication of private words or images without consent. French courts have applied this article in cases of *revenge porn*, often resulting in convictions that address the privacy violation aspect of digital abuse, though such single-act offences differ from sustained cyberbullying.[4] Oman similarly criminalises privacy violations under Articles 330 and 332 of the Penal Code and Article 16 of the Cybercrime Law, penalising unauthorised disclosure of private information.

Acts such as publishing a victim's private images or altered photos fall within these offences, especially where personal identity is distorted (Khalafi, 2011). The Omani Supreme Court affirmed this in Appeals 908/2015 and 909/2015, involving a husband who sent intimate images of his wife via WhatsApp.

Despite overlaps, cyberbullying remains distinct. Privacy offences may be consummated by a single act and protect personal autonomy and confidentiality, whereas cyberbullying requires repetition and protects emotional security and psychological integrity.

3. Cyberbullying and the Offence of Threatening Behaviour While US federal law lacks a unified "cyberbullying" offence, statutes such as 18 U.S.C. § 875 criminalise interstate communications

[2] *People v. Marquan M.*, 19 N.Y.3d 981 (N.Y. 2014). In this case, the New York Court of Appeals analyzed a local cyberbullying statute. While the statute was struck down on vagueness grounds, the court's reasoning highlighted that the prohibited conduct was understood as a repeated, targeted course of action intended to inflict significant emotional distress, thereby underscoring the specific intent and cumulative harm characteristic of cyberbullying, as opposed to the single publication and reputational focus of defamation law.

[3] In March 2024, a man was convicted under the new "cyber-flashing" provision (Online Safety Act 2023) for sending unsolicited explicit images. This case illustrates the UK's targeted approach to criminalising specific digital sexual harassment, a behaviour often presents within broader cyberbullying campaigns but treated here as a discrete offence focusing on the intrusive act rather than a pattern of psychological abuse.

[4] See, for instance, Cour d'appel de Paris, Pôle 2 - Chambre 11, Arrêt du 7 septembre 2022 (No. 21/00804), where the defendant was convicted under Article 226-1 for disseminating private intimate images without consent. The conviction addressed the violation of privacy and image rights, distinct from a cyberbullying charge which would require evidence of a repeated course of conduct intended to cause psychological harm.

containing threats of injury or extortion. In *Elonis v. United States*, the Supreme Court reversed a conviction for threats made via Facebook rap lyrics, holding that the prosecution must prove subjective *mens rea*—that the defendant consciously disregarded a substantial risk of his statements being interpreted as threats (*Elonis v. United States*, 575 U.S. 723, 2015).

In France, Article 222-18 of the Penal Code criminalises threats accompanied by an order. In Oman, Article 324 of the Penal Code and Article 18 of the Cybercrime Law criminalise threats through any medium, electronic or otherwise.

Jordanian jurisprudence provides a relevant analogy; in Decision No. 9-5/2019, the Court of Cassation upheld a conviction where the accused filmed the victim nude and threatened disclosure (Al-Ubaydi & Al-Mashhadani, 2022).

The distinction lies in the protected interest: threat offences protect personal liberty and security, whereas cyberbullying protects psychological well-being. Some US states differentiate cyberbullying from standard threats by imposing specialised penalties on students who create hostile digital environments, such as under the California Safe Place to Learn Act and Missouri anti-harassment provisions (Al-Najjar, 2020). For instance, California's law focuses on sustained conduct that creates a hostile educational environment, moving beyond the single threatening statement.[5]

4. Cyberbullying and Offences Involving Unlawful Access, Data Interference, and Misuse of Information Technologies Misuse of the information network and its technologies, and violation of the confidentiality of electronic information and data stored in it, poses a great danger that threatens the lives of individuals and society, which may have a very bad effect and harm users or the general order in society (Alhoussari, 2025). In the United States, the Computer Fraud and Abuse Act (18 U.S.C. § 1030) penalises unauthorised access to protected computers and causing damage through digital transmissions. Omani law similarly protects data and system integrity under Article 3 of the Cybercrime Law, with enhanced penalties for personal data breaches. Article 11 criminalises creating or disseminating tools for cybercrimes.

These offences, however, focus on the integrity, confidentiality, and security of information systems, not on harmful content directed at an individual. Thus, while cyberbullying may employ digital tools, criminalising system misuse does not address the psychological and emotional harm central to cyberbullying.

Iraqi jurisprudence illustrates this distinction: the Karkh Criminal Court convicted a hacking network under Article 430 of the Penal Code for extortion involving stolen images, because they took photos and copied electronic conversations, then blackmailed their owners and threatened to publish them on all websites if they did not pay, with the intent to defame, threaten, and extort (Hanash, 2020).

5. Cyberbullying and the Offences of Discrimination and Hate Speech States increasingly criminalise discrimination and hate speech to protect social cohesion and equality (Abdelaziz, 2025b). In the United States, the Hate Crimes Prevention Act (18 U.S.C. § 249) criminalises bodily injury motivated by race, colour, religion, or national origin (18 U.S.C. § 249, 2025). French Penal Code Article 225-1 defines discrimination based on origin, sex, disabilities, etc., and Article 225-2 criminalises related threats or harassment. The UK Equality Act 2010 and Public Order Act 1986 similarly criminalise discriminatory conduct and hate incitement.

Oman safeguards equality and prohibits conduct threatening national unity under Articles 15, 21, and 37 of the Basic Law, while Article 108 of the Penal Code criminalises incitement of hatred or social discord.

Although discriminatory harassment may resemble cyberbullying, key distinctions persist. First, discrimination offences may target a specific individual or a protected class, whereas cyberbullying targets a specific victim. Second, discrimination may be completed by a single act; cyberbullying requires repetition. Third, discrimination protects equality and public order, whereas cyberbullying protects personal emotional well-being.

Some jurisdictions have enacted specialised legislation for discriminatory cyberbullying. France adopted Law No. 2020-766 on combating hateful online content, and the UAE enacted Federal Law No. 2 of 2015 on Combating Discrimination and Hatred. In the United States, discriminatory harassment in schools is governed by federal civil rights statutes where severe behaviour creates a hostile environment (Al-Ubaydi & Al-Mashhadani, 2022).

In sum, while cyberbullying shares several

[5] California Education Code § 234.1 (Safe Place to Learn Act) requires schools to adopt policies against discrimination, harassment, intimidation, and bullying. Enforcement focuses on patterns of behaviour that create a hostile environment, moving beyond punishing single threats to address sustained psychological harm in educational settings, aligning closely with the structural nature of cyberbullying.

external manifestations with adjacent offences such as defamation, privacy violations, threats, system misuse, and discriminatory speech, it nonetheless exhibits a constellation of distinctive elements—special intent, repetition, technological power imbalance, and directed psychological harm—that justify its treatment as an autonomous offence rather than a mere extension of existing criminal categories. These distinctions set the conceptual foundation for the concluding section, which synthesises the comparative analysis and evaluates the broader implications for legislative reform.

4. CONCLUSION

This study has examined the criminal law response to cyberbullying through a comparative analysis of the legal frameworks of Oman, the United States, the United Kingdom, and France. The core finding is the doctrinal necessity of recognising cyberbullying as a punishable act in its own right. Criminalisation does not conflict with freedom of expression, as cyberbullying infringes upon more compelling legal interests—namely psychological integrity, equality, and the preservation of human dignity. These interests justify imposing liability for repeated, targeted, and harm-inflicting digital conduct.

From the comparative study, several key findings emerge First, cyberbullying possesses distinctive characteristics that differentiate it from related offences such as defamation, privacy violations, threats, data misuse, and hate-motivated conduct. These features include special intent, behavioural repetition, and the exploitation of technological asymmetry between perpetrator and victim.

Second, jurisdictions differ sharply in their legislative strategies. The analysis reveals a fragmented regulatory landscape. At the federal level, the United States lacks an explicit statutory offence labelled "cyberbullying," although forty-nine out of fifty states currently criminalise the behaviour to varying degrees, with significant discrepancies in definitions, scope, and sanctions. [For instance, while California and New York have specific statutes, their definitions and scopes differ, illustrating the lack of uniformity.[6] Similarly, the United Kingdom has not enacted a specific "cyberbullying" offence, relying instead on a patchwork of statutes like the Malicious Communications Act 1988 and the Online Safety Act 2023. France represents a more integrated approach, criminalising specific types of harassment across contexts with aggravated penalties for online commission, while Oman lacks explicit provisions altogether, addressing conduct indirectly through general penal and cybercrime laws.

Third, the severity of sanctions varies considerably. Comparative legislation ranges from misdemeanour-level penalties to felony-grade sanctions when cyberbullying results in severe physical or psychological harm, or where aggravating circumstances are present.

Fourth, a significant legislative gap persists. Existing cybercrime and penal provisions in the surveyed jurisdictions do not sufficiently encompass the full spectrum of cyberbullying behaviours—such as impersonation, digital exclusion, persistent unsolicited contact, humiliation, or technologically-facilitated harassment. This underscores the need for targeted reform.

In light of these findings, **the study proposes several recommendations**

- For the United States: Adoption of a clear federal statute providing a uniform definition of cyberbullying, harmonising state-level discrepancies while balancing criminal liability with First Amendment protections.
- For Oman, the United Kingdom, and France: Enactment or refinement of dedicated legislation that clearly defines the offence, its constituent elements, and establishes proportionate penalties.
- For all jurisdictions: The recommended statute should provide for graduated aggravating circumstances (e.g., involving minor victims, suicide, or abuse of authority) and authorise supplementary judicial measures, such as account closure orders, no-contact directives, and mandated psychological rehabilitation.

Furthermore, the criminal justice response must be supported by specialised training for law-enforcement and judicial bodies in digital-evidence preservation and the psychological dimensions of online harm.

In conclusion, cyberbullying should not be viewed solely as a criminal phenomenon. A holistic strategy is required—combining precise criminal accountability with preventive educational programmes, technological safety measures, and community-based interventions—to protect

[6] Compare California Penal Code § 653.2 (focusing on electronic harassment intended to place a person in fear for their safety) with New York Education Law § 12-d (focusing on harassment and bullying of students by students via electronic means). This disparity highlights the challenges of a state-by-state approach and the practical need for a coherent federal definition to guide enforcement and policy.

psychological well-being, human dignity, and social harmony in the digital era.

Acknowledgments: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

REFERENCES

Abdelaziz, D. K. A. (2025a). Incitement to suicide in the digital age: A comparative legal study of criminal liability. *Journal of Posthumanism, 5*(6), 684–699. https://doi.org/10.63332/joph.v5i6.2105

Abdelaziz, D. K. A. (2025b). Between justice and hidden intent: Proving hate crimes in comparative law. *Journal of Ecohumanism, 3*(8), 10376. https://doi.org/10.62754/joe.v3i8.5648

Al-Harbi, J. (2019). 'Cyberbullying… Hostile behaviour to damage reputation.' *Al-Riyadh Newspaper.* https://www.alriyadh.com/1784694

Alhoussari, H. (2025). Securing health data in the digital age: Challenges, regulatory frameworks, and strategic solutions in Saudi Arabia. *Journal of Ecohumanism, 4*(1), 2310. https://doi.org/10.62754/joe.v4i1.6052

Al-Khasawneh, S. A. (2020). Adequacy of electronic legislation in limiting cyberbullying: A study in Jordanian law. *International Journal of Comparative Legal Studies.*

Al-Najjar, S. F. (2022). The position of the United States on cyberbullying. https://almerja.net/reading.php?idm=154867

Al-Najjar, S. F. M. (2020). Cyberbullying crime: A comparative study in Iraqi and American law. *Academic Journal of Legal Research, 11*(4), 134–166.

Alomar, A. M., & Alabady, H. (2023). The phenomenon of cyber bullying: Interpretation, confrontation, and the position of Islamic law. *Journal of Namibian Studies, 34*, 746–768. https://namibian-studies.com/index.php/JNS/article/view/1123/872

Al-Tayyar, A. A. (2022). The crime of bullying: A comparative study. Dar al-Jami'a al-Jadida.

Al-Tuni, Kh. M. (2016). Criminal confrontation of cyberbullying in comparative criminal legislation. *Journal of the Faculty of Shari'a and Law, 31*(1), 10–168. Tanta University.

Al-Ubaydi, U. A., & al-Mashhadani, B. A. (2022). Cyberbullying crime. Arab Center for Publishing and Distribution. American Library Association. (2021). Censorship and intellectual freedom. https://www.ala.org/advocacy/intfreedom/censorship

BBC News. (2024, March 20). Cyber-flashing "Not a Joke", warns CPS prosecutor.

Bethel School District No. 403 v. Fraser, 478 U.S. 675 (1986).

Bozbayindir, G. B. (2019). Cyberbullying and criminal law. *Istanbul Law Review, 77*(1), 425–450. https://doi.org/10.26650/mecmua.2019.77.1.0009

Channak, Z. (2026). *The Saudi criminal law – General part: Theory of crime and punishment* (11th ed.). Dar al-Kitab al-Jamee Library. Communications Act 2003 (United Kingdom).

Cour de cassation, chambre criminelle, Arrêt n° 04-86.507 (12 July 2005). https://www.legifrance.gouv.fr/juri/id/JURITEXT000007608419

Ditch the Label. (2013). The annual cyberbullying survey 2013 [PDF]. https://www.scribd.com/document/172506985/Ditch-the-Label-The-Annual-Cyberbullying-Survey-2013

Elonis v. United States, 575 U.S. 723 (2015).

Equality Act 2010 (United Kingdom).

Ferguson, M. (2014). Should cyberbullying be a crime?

Flavi, B. (2017). Is cyberbullying illegal? When comments turn criminal. Rasmussen University. https://www.rasmussen.edu/degrees/justice-studies/blog/is-cyberbullying-illegal/

Hallmark, K. (2023). Death by words: Do United States statutes hold cyberbullies liable for their victims' suicide? *Houston Law Review, 60*, 727.

Legal Information Institute. (2022). First Amendment. Cornell Law School. https://www.law.cornell.edu/wex/first_amendment

Loi n° 2014-873 du 4 août 2014 (France).

Malicious Communications Act 1988 (United Kingdom). Online Safety Act 2023 (United Kingdom). https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted

Public Order Act 1986 (United Kingdom).

United States v. Alvarez, 567 U.S. 709 (2012).

United States Code, Office of the Law Revision Counsel. https://uscode.house.gov
18 U.S.C. § 875 (Interstate Communications) (2024).
18 U.S.C. § 1030 (Fraud and Related Activity in Connection with Computers) (2025).
18 U.S.C. § 249 (Hate Crimes Prevention Act).