

An Analysis of the Legal and Human Rights Protection for Cyberbullying for Athletes in Malaysia

Thieveeya Krishnan¹, Yamunaa Nyanasekaran², Maheran Makhtar³

¹ Faculty of Law and International Relations, Universiti Sultan Zainal Abidin, Malaysia

Corresponding Author: maheranmakhtar@unisza.edu.my

ARTICLE INFO

Article History

Received: March 10, 2026

Revised: July 20, 2026

Accepted: August 11, 2026

Keywords

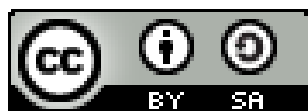
Cyberbullying;

Legal Protection;

Human Rights Law;

Athletes

This is an open-access article
under the CC-BY-SA license.



ABSTRACT

This study critically evaluates the efficacy of Malaysia's statutory and human rights frameworks in safeguarding athletes against the rising tide of cyberbullying and online abuse. Operating within a high-performance environment where performative toxicity and performance-triggered vitriol are prevalent, athlete protection remains severely hindered by statutory fragmentation, legislative ambiguity, and inadequate procedural mechanisms. The primary catalyst for this research stems from critical legislative gaps, specifically, the lack of explicit statutory definitions for the terms bullying and cyberbullying, combined with inadequate penal sanctions and fragmented procedural mechanisms. Employing a mixed doctrinal and qualitative empirical methodology comprising statutory critique, comparative legal analysis against statutory models in Singapore and Australia, and semi-structured interviews with 16 national athletes, this paper exposes major structural defects in existing Malaysian legislation, including the Communications and Multimedia Act (CMA) 1998, Penal Code, Minor Offenses Act 1955, Defamation Act 1957 and Evidence Act 1950. Singapore and Australia were selected as comparative jurisdictions due to their advanced, purpose-built legal frameworks governing cyberbullying and digital harm... The findings demonstrate that Malaysia's existing legal framework remains inadequate in addressing the complex realities of cyberbullying, with empirical evidence from 16 national athletes revealing significant emotional, psychological, and professional consequences arising from digital harassment, thereby highlighting the urgent need for a more coherent and rights-based regulatory framework.

Introduction

The rapid proliferation of digital communication technologies and social media platforms has radically transformed the landscape of modern sports engagement. While online networks provide athletes with unprecedented opportunities for personal branding, fan interaction, and commercial sponsorship, they simultaneously expose sports professionals to unprecedented levels of cyberbullying, targeted harassment, and digital abuse.¹ Unlike traditional workplace or athletic bullying, which typically occurs within defined physical spaces and operating hours,

¹ Adamu Gaston Philipo et al., "Cyberbullying Detection: Exploring Datasets, Technologies, and Approaches on Social Media Platforms," *ACM Computing Surveys* 58, no. 7 (May 2026): 1–35, <https://doi.org/10.1145/3785654>.

cyberbullying operates without spatial or temporal limitation.² Perpetrated anonymously and amplified exponentially through viral algorithms, digital toxicity follows athletes continuously into their private lives, inflicting severe psychological distress and damaging professional livelihoods.³

In Malaysia, escalating online harassment has become a national concern. Statistical data from the Ministry of Education shows a dramatic surge in reported bullying incidents, rising from 326 cases in 2021 to 3,887 in 2022, 4,994 in 2023, and 6,208 in 2024.⁴ Furthermore, international comparative metrics published by UNICEF ranked Malaysia second in Asia for youth cyberbullying.⁵ In response to widespread digital hostility, the Malaysian Communications and Multimedia Commission (MCMC) removed 27,704 cyberbullying-related posts out of 35,781 formal complaints logged between January and October 2025 alone.⁶ Social media platform complaints were predominantly concentrated on Facebook (1,401), followed by WhatsApp (667), Instagram (338), TikTok (258), and X (159).⁷

Table 1. Escalation of Reported Bullying Statistics in Malaysia (2021–2024)

Year	Total Reported Cases
2021	326
2022	3887
2023	4994
2024	6208

Source: *Compiled by the author based on several references*

Despite these alarming metrics, Malaysia’s legal landscape lacks a dedicated, unified statutory framework governing cyberbullying. Current enforcement relies upon a fragmented mosaic of legacy statutes, including the Penal Code (Act 574), Communications and Multimedia Act (CMA) 1998, Minor Offenses Act 1955, Defamation Act 1957, and Evidence Act 1950. This legal fragmentation creates substantial substantive and procedural barriers to enforcement. Existing laws fail to provide a precise statutory definition for ‘cyberbullying’ or codify its essential

² Sangmi Kim et al., “The Evolution of Cyberbullying Definitions in the Digital Age: A Systematic Review of Defining Attributes and Conceptual Synthesis,” *Journal of Technology in Human Services*, March 2026, 1–31, <https://doi.org/10.1080/15228835.2026.2647023>.

³ Kevin Dixon, “Content Leakage: Privacy, Exposure and the Athlete in the Public Eye,” in *Combating Online Abuse in Sports* (Cham: Springer Nature Switzerland, 2026), 37–63, https://doi.org/10.1007/978-3-032-17822-0_3.

⁴ James O’Higgins Norman et al., “School Bullying: Moving beyond a Single School Response to a Whole Education Approach,” *Pastoral Care in Education* 40, no. 3 (July 2022): 328–41, <https://doi.org/10.1080/02643944.2022.2095419>.

⁵ Willone Lim et al., “Sociodemographic Factors Associated with Cyberbullying Experience and Practice Among Youths in Malaysia,” *Journal of Technology in Behavioral Science* 10, no. 3 (December 2024): 613–23, <https://doi.org/10.1007/s41347-024-00469-9>.

⁶ Jasmeen Kah Ying Bong, Kasturi Dewi Varathan (Corresponding Author), and Teoh Hwai Teng, “Cyberbullying Detection In Social Media Using Pre-Trained Language Models,” *Malaysian Journal of Computer Science* 38, no. 1 (December 2025): 29–54, <https://doi.org/10.22452/mjcs.vol38no1.2>.

⁷ Isadora Mendes Dos Santos et al., “Social Media for Whom? The Absence of Guideline Adherence in Social Platforms,” *IEEE Access* 14 (2026): 53360–77, <https://doi.org/10.1109/Access.2026.3680543>.

criminal elements (*actus reus* and *mens rea*). Consequently, law enforcement authorities and prosecutors are frequently constrained to apply generic or disproportionately lenient provisions.⁸ A tragic illustration occurred in 2024, when a perpetrator whose online trolling directly drove a prominent Malaysian social media influencer to suicide was sentenced under Section 14 of the Minor Offences Act 1955 to a maximum statutory fine of merely RM100, a penalty grossly disproportionate to the loss of human life.⁹

In the domain of high-performance sports, Malaysian athletes face heightened vulnerability to cyberbullying. Elite athletes operate in public-facing, high-stakes environments where athletic errors or underperformance during major tournaments (such as the Olympic Games or SUKMA) routinely trigger coordinated campaigns of online hate, xenophobic insults, and physical threats. Existing general legal remedies fail to offer fast-tracked protection or address the unique career vulnerabilities of sports professionals.

Accordingly, this study conducts a rigorous legal and empirical examination of cyberbullying protection for Malaysian athletes. While existing literature focuses predominantly on youth- or school-based cyberbullying under general penal provisions, this study uniquely bridges legal analysis with empirical sports science. Specifically, it evaluates Malaysia's current legislative framework, examines the psychological and professional impacts through qualitative empirical data from 16 national athletes, compares Malaysian laws against advanced statutory regimes in Singapore and Australia, and formulates actionable, sports-specific legislative reforms to establish a robust protective framework.

Methods

This research employed doctrinal legal research and qualitative research through semi-structured interviews.¹⁰ Doctrinal legal research will focus on the text and principles of the law, providing a thorough examination of legal norms from primary sources such as statutes and court judgments.¹¹ This analysis will specifically cover the Communications and Multimedia Act (CMA) 1998, the Penal Code (Act 574), the Minor Offences Act 1955, the Defamation Act 1957, the Evidence Act 1950, as well as Article 10 of the Federal Constitution. Furthermore, a legal analysis of pertinent cyberbullying statutes from Singapore and Australia will be conducted

⁸ Liubomir Nikiforov, "The Law Enforcement Directive 2016/680 in Practice: Transparency, Lawfulness and Strict Necessity. Lessons from Bulgaria," *Computer Law & Security Review* 62 (September 2026): 106370, <https://doi.org/10.1016/j.clsr.2026.106370>.

⁹ Sarmini, "From Memes to Harassment Automated Detection of Cyberbullying for Cyberlaw Enforcement," *Journal of Cyber Law* 1, no. 4 (December 2025), <https://doi.org/10.63913/jcl.v1i4.3>.

¹⁰ Nurazlina Abdul Raof et al., "Exploring the Depths: A Comparative Analysis of Doctrinal and Non-Doctrinal Legal Research," *International Journal of Research in Social Science and Humanities* 06, no. 05 (2025): 122–29, <https://doi.org/10.47505/IJRSS.2025.5.13>.

¹¹ Nasir Majeed, Amjad Hilal, and Arshad Nawaz Khan, "Doctrinal Research in Law: Meaning, Scope and Methodology," *Bulletin of Business and Economics (BBE)* 12, no. 4 (December 2023): 559–63, <https://doi.org/10.61506/01.00167>.

to benchmark current Malaysian legislation.

The qualitative approach deeply explored and investigated the concepts, situations, and experiences related to the effect of cyberbullying on athletes.¹² Qualitative research is suitable because it focuses on the ‘how’ and ‘why’ of phenomena, providing a profound understanding of the subject matter.¹³ The qualitative method is preferred as the primary data collected from athlete interviews will yield non-numerical answers.¹⁴ This approach also allows for flexible reporting that accommodates the nature of the data. Interview data will serve as the primary data source because it is reliable and accurate when administered to the targeted athletes. This method involves two-way communication to gather qualitative data, which includes information that cannot be measured or counted numerically. Specifically, unstructured, open-ended interviews will be used to allow athletes the freedom to fully elaborate on their experiences with cyberbullying and its psychological and professional effects. The target group comprises 16 athletes selected based on race, achievement level, and sport to provide a well-rounded perspective. This sample size aligns with qualitative research norms, which often suggest 12 to 20 interviews for maximal variability in a heterogeneous sample.¹⁵ Considering the diversity of participants and the complexity of cyberbullying, 16 respondents are sufficient to capture a comprehensive understanding of the issue. Interviews will be conducted online following major sports events such as the Paris Olympics 2024 and Sukan Malaysia (SUKMA) 2024, using open-ended questions aligned with the research objectives. The interview data will be analyzed using thematic analysis to identify, analyze, and report patterns or themes within the dataset.¹⁶ This process involves transcription of recordings, coding, and theming, which ultimately helps researchers systematically organize complex qualitative data.¹⁷

¹² Faye Mishna, Arija Birze, and Andrea Greenblatt, “Understanding Bullying and Cyberbullying Through an Ecological Systems Framework: The Value of Qualitative Interviewing in a Mixed Methods Approach,” *International Journal of Bullying Prevention* 4, no. 3 (September 2022): 220–29, <https://doi.org/10.1007/s42380-022-00126-w>.

¹³ Weng Marc Lim, “What Is Qualitative Research? An Overview and Guidelines,” *Australasian Marketing Journal* 33, no. 2 (May 2025): 199–229, <https://doi.org/10.1177/14413582241264619>.

¹⁴ David Tod, Samuel Pullinger, and Moira Lafferty, “A Systematic Review of the Qualitative Research Examining Stakeholders’ Perceptions of the Characteristics of Helpful Sport and Exercise Psychology Practitioners,” *International Review of Sport and Exercise Psychology* 17, no. 2 (December 2024): 1312–36, <https://doi.org/10.1080/1750984X.2022.2145575>.

¹⁵ Monique Hennink and Bonnie N. Kaiser, “Sample Sizes for Saturation in Qualitative Research: A Systematic Review of Empirical Tests,” *Social Science & Medicine* 292 (January 2022): 114523, <https://doi.org/10.1016/j.socscimed.2021.114523>.

¹⁶ Manuel Goyanes, Carlos Lopezosa, and Beatriz Jordá, “Thematic Analysis of Interview Data with ChatGPT: Designing and Testing a Reliable Research Protocol for Qualitative Research,” *Quality & Quantity* 59, no. 6 (December 2025): 5491–5510, <https://doi.org/10.1007/s11135-025-02199-3>.

¹⁷ Jayne Njeri Mugwe and Steven Runo, “Qualitative Data Analysis,” in *Research Methodology in Agricultural Sciences* (Singapore: Springer Nature Singapore, 2026), 561–83, https://doi.org/10.1007/978-981-95-1892-0_23.

Discussion

Legal Framework on Cyberbullying in Malaysia

Article 10(1)(a) guarantees every citizen the fundamental right to freedom of speech and expression. However, this right is non-absolute. Under Article 10(2)(a) and Article 10(4), Parliament retains constitutional authority to impose statutory restrictions in the interests of security, public order, morality, protection against defamation, or incitement to any offense. The challenge in drafting anti-cyberbullying legislation lies in establishing proportionate statutory boundaries that curtail malicious harassment without infringing upon legitimate, constitutionally protected public criticism. The Federal Court in the case of *Chong Chieng Jen v Government of State of Sarawak & Anor* [2019] 3 MLJ 300, the Federal Court stated that ‘in Malaysia the freedom of speech is provided under article 10 of the Federal Constitution. That right is not absolute or unfettered. It is clear that while the right of freedom of speech is guaranteed under article 10(1)(a) of the Federal Constitution, article 10(2)(a) has imposed restrictions by authorizing Parliament to enact laws it deems necessary to provide for defamation, or incitement to any offense.’¹⁸ Under constitutional jurisprudence, any statutory limitation imposed on the fundamental right to freedom of speech and expression must satisfy the standard of reasonableness. Courts evaluate reasonableness through a structured proportionality test, examining whether the legislative restriction is strictly necessary to achieve a legitimate state objective, whether the measure is proportional to the harm targeted, and whether less restrictive alternatives could effectively attain the same legislative goal as illustrated in *Amir Hariri Bin Abd Hadi v Public Prosecutor* [2025] 4 MLJ 807.

Currently, Malaysia lacks a dedicated, standalone statutory framework governing cyberbullying. Instead, digital harassment is addressed through a fragmented matrix of existing legislation, including the Communications and Multimedia Act (CMA) 1998, the Penal Code (Act 574), the Minor Offenses Act 1955, the Defamation Act 1957, and the Evidence Act 1950.¹⁹ In the absence of specialized legislation, authorities rely on these general enactments to establish legal accountability for online misconduct.

1) *Communications and Multimedia Act (CMA) 1998*

The primary statutory instrument applied to digital misconduct is Section 233 of the CMA 1998, which criminalizes the improper use of network facilities or application services. Specifically, Section 233(1)(a) penalizes transmitting communications that are obscene, indecent, false, menacing, or grossly offensive

¹⁸ Tryan Zaki Aulia Yanis et al., “The Unconstitutionality of the Offence of Insulting the Government in the 2023 Criminal Code: A Critical Review of Freedom of Expression,” *As-Siyasi: Journal of Constitutional Law* 5, no. 1 (June 2025): 111–19, <https://doi.org/10.24042/as-siyasi.v5i1.24739>.

¹⁹ Subhajit Basu and Shameek Sen, “Silenced Voices: Unravelling India’s Dissent Crisis through Historical and Contemporary Analysis of Free Speech and Suppression,” *Information & Communications Technology Law* 33, no. 1 (January 2024): 42–65, <https://doi.org/10.1080/13600834.2023.2249780>.

with intent to annoy, abuse, threaten, or harass another person. Amendments proposed under the Communications and Multimedia (Amendment) Bill increase statutory penalties to a fine of up to RM 500,000, imprisonment of up to two years, or both. The elements the prosecutor must prove are *actus reus*: making, creating, soliciting, or initiating the transmission of content via network/application services, and *mens rea*: intent to *annoy, abuse, threaten, or harass* another person. The provision lacks objective definitions for what constitutes ‘grossly offensive’ content or ‘intent to annoy’. Defense counsel frequently challenge charges by asserting that the communication was merely harsh public criticism, satire, or protected speech under Article 10(1)(a) of the Federal Constitution. Thus, the prosecutors bear the heavy burden of establishing beyond reasonable doubt that the offender possessed the *specific intent* to harass or annoy, rather than merely venting frustration or expressing an opinion online. While Section 233 carries substantial criminal penalties (up to RM500,000 fine or 2 years imprisonment), it is a *punitively reactive* criminal provision. It does not grant prosecutors or courts administrative powers to issue immediate 24-hour takedown orders or interim protection orders to shield victims while criminal trials linger. Despite its widespread application, Section 233 CMA suffers from critical statutory deficiencies. Legal scholars highlight that Section 233 is frequently invoked to prosecute general political dissent or satirical commentary rather than targeted interpersonal cyberbullying.²⁰

2) Penal Code (Act 574)

The Penal Code (Act 574) serves as the primary statutory framework codifying substantive criminal offenses in Malaysia. Although cyberbullying is not explicitly defined or classified as a standalone offense under the Code, several existing provisions are frequently invoked to address digital harassment. Several Penal Code sections are extended to digital offenses:

- a) Section 499 (Criminal Defamation): Requires proving beyond a reasonable doubt that the bully made a false imputation intending to harm the victim's reputation. The standard of proof in criminal defamation is exceptionally high, and prosecutors rarely pursue online trolling under Section 499 due to procedural complexity and prolonged trial timelines.
- b) Section 503 (Criminal Intimidation): Invoked when an online bully threatens a victim with harm to their person, reputation, or property. Section 503 was drafted with physical threats in mind. It struggles to encompass modern cyberbullying modalities such as doxxing (publishing personal address/phone numbers to invite public harassment), online impersonation, or algorithmic swarming, where no direct physical threat is explicitly stated
- c) Section 507A (Anti-Stalking): Enacted in 2023, Section 507A criminalizes repeated acts of physical or online harassment intended to cause distress, fear, or alarm regarding safety. It provides a vital legal tool against persistent

²⁰ Basu and Sen.

online stalkers and allows victims to apply for temporary Protection Orders. It requires strict proof of "repeatedly" (statutorily interpreted as at least two distinct occasions). Consequently, a single, high-intensity viral harassment event—such as a single post that receives thousands of hostile shares driving an athlete or individual to severe distress—cannot be prosecuted under Section 507A.

- d) Section 509: Historically, Section 509 has been invoked to prosecute acts—including verbal remarks, gestures, and digital messages or posts—that insult the modesty of a person or intrude upon privacy. Before recent anti-bullying and anti-stalking amendments to the Penal Code (such as Section 507A for stalking and Sections 507B–507G for harassment/bullying), Section 509 was one of the few provisions used to target gender-based digital harassment, online shaming, or privacy invasions. Prosecuting under Section 509 requires establishing that the offender specifically possessed the intent (*mens rea*) to "insult the modesty" or "intrude upon the privacy" of a person. It does not, however, encompass general non-gendered performance harassment, doxxing, or collective digital swarming unless those acts fall within modesty or privacy invasions.

Although these penal provisions do not explicitly define cyberbullying, they remain legally applicable to various forms of online abuse. For example, Section 503 of the Penal Code governs criminal intimidation and applies directly when a perpetrator transmits threatening digital messages such as extortion demands or threats against a victim's family via social media platforms. Similarly, criminal defamation under Section 499 penalizes individuals who publish or share defamatory content using digital devices. In the civil sphere, digital publication is governed under equivalent common law principles, as demonstrated in *Abu Hassan bin Hasbullah v. Zukeri bin Ibrahim* [2018] 6 MLJ 396. In that case, the Court of Appeal overturned the High Court's ruling, holding that slanderous emails sent to university staff were inherently defamatory, thereby establishing that electronic communications fulfill the legal requirement of publication.

Furthermore, Section 507A of the Penal Code explicitly addresses persistent physical and digital stalking.²¹ This provision allows the prosecution of cyberbullies who engage in repeated online harassment, provided the conduct occurs on at least two distinct occasions to satisfy the statutory threshold of "repeatedly." However, prosecuting cyberstalking under Section 507A presents significant evidentiary hurdles. Perpetrators frequently utilize anonymous pseudonyms, false profiles, or multiple social media accounts to evade detection, making it exceptionally difficult for law enforcement and prosecutors to establish the offender's identity beyond a reasonable doubt.

²¹ Sanskriti Gautam, "Freedom of Speech and Expression: Responses to Online Harassment," 2025, <https://doi.org/10.2139/ssrn.5210246>.

3) *Minor Offenses Act 1955*

In the absence of a dedicated statutory framework, the Minor Offenses Act 1955 has increasingly functioned as a prosecutorial fallback in cyberbullying cases where higher evidentiary burdens under specific telecommunications or penal statutes cannot be satisfied. Enacted primarily to regulate low-level public disturbances, this legacy statute prescribes minimal punitive measures. The provision most directly extended to online abuse is Section 14, which criminalizes the use of indecent, threatening, abusive, or insulting words or behavior likely to provoke a breach of the peace. However, relying on Section 14 to address severe digital toxicity exposes critical enforcement gaps, as its statutory maximum penalty is restricted to a nominal fine of RM100.

The manifest inadequacy of this statutory penalty was demonstrated in the high-profile cyberbullying case of social media influencer Esha (Rajeswary Appahu).²² Despite the perpetrator engaging in systematic online trolling that directly contributed to the victim's tragic suicide, the prosecution was constrained to invoke Section 14 of the Minor Offenses Act 1955 due to legislative gaps, resulting in a maximum fine of merely RM100. This outcome underscores a profound *lacuna* in Malaysian jurisprudence, where legacy public nuisance laws fail to reflect the severe psychological devastation and fatal consequences of modern cyber-victimization. A nominal financial penalty trivializes victim suffering, compromises judicial proportionality, and severely undermines both the deterrent and retributive functions of criminal law.

4) *Defamation Act 1957*

The law of defamation in Malaysia is rooted in English common law principles, with the Defamation Act 1957 modeled in *pari materia* after the English Defamation Act 1952. Because the Act does not explicitly define defamation, Malaysian courts adopt the common law standard—namely, that a statement is defamatory if it tends to lower a person in the estimation of right-thinking members of society generally, or causes them to be shunned or avoided (*Parmiter v. Coupland* [1840] 6 M&W 105). The 1957 Act underpins civil remedies for both libel (permanent digital or written form) and slander (temporary form).²³

An analysis of Sections 3, 4, 5, and 6 of the Malaysian Defamation Act 1957 in the context of cyberbullying reveals how traditional civil law provisions apply to modern digital harassment. Although the Defamation Act 1957 was drafted long before the internet age, these provisions remain a primary civil remedy for victims seeking monetary compensation (damages) and court injunctions (takedown orders)

²² Meruert Rakymbaeva et al., “Cyberbullying of Minors and Juvenile Justice: Digital Evidence and Chain-of-custody in Suicide Incitement Cases,” *Juvenile & Family Court Journal*, July 2026, <https://doi.org/10.1111/jfcj.70031>.

²³ Hayleigh Boshier, “Do Deepfakes, Digital Replicas and Human Digital Twins Justify Personality Rights?,” *The Journal of World Intellectual Property*, March 2026, <https://doi.org/10.1111/jwip.70020>.

against cyberbullies.

- a) Section 3: Section 3 treats words broadcast via telecommunication or radio communication as publication in permanent form (libel) rather than temporary form (slander). Libel is actionable *per se*, meaning the victim does not need to prove actual financial/pecuniary loss to win the case. Modern Malaysian courts interpret internet posts, social media comments, live streams, emails, and messaging apps (WhatsApp/Telegram) as permanent communications (libel) as per *Tony Pua Kiam Wee v Dato' Sri Mohd Najib bin Tun Haji Abdul Razak* [2018] 3 CLJ 522. Because cyberbullying posts are treated as libel under Section 3, victims targeting online bullies do not have to prove specific financial loss. The law automatically presumes reputational and emotional injury once defamatory publication to a third party is established.
- b) Section 4: Imputing unchastity or adultery to any woman or girl is an exception to general slander rules and is actionable *per se* without proving special damages. Cyberbullying frequently manifests as gender-based harassment, "slut-shaming," non-consensual sharing of intimate insinuations, or character assassination targeting women and girls online. Even if a bully attempts to argue that their online statement was transient or oral (e.g., voiced during a live stream or voice note), Section 4 ensures female victims have an automatic right of action without needing to prove financial injury.
- c) Section 5: Statements calculated to disparage a person in any office, profession, calling, trade, or business held at the time of publication are actionable *per se*. Online bullies frequently target high-profile individuals—such as national athletes, coaches, public figures, or business owners—by falsely accusing them of unfitness, corruption, cheating, match-fixing, or incompetence. Section 5 allows these targeted individuals to sue cyberbullies directly for reputational damage to their career or brand without having to quantify exact lost sponsorship earnings at the initial stage of litigation.
- d) Section 6: Eliminates the requirement to prove special damage if malicious statements published in permanent form are calculated to cause financial/pecuniary damage to a person's trade, business, or profession. Protects victims against organized online boycott campaigns, false reviews, or malicious rumors aimed at destroying an individual's commercial livelihood, endorsement deals, or personal branding.

Although the Defamation Act 1957 contains no explicit reference to cyberbullying, its expansive statutory scope allows defamation law to encompass digital harassment that harms personal or professional reputation. Conceptually, cyberbullying and defamation overlap when an offender publishes false or derogatory statements online intended to subject a victim to public hatred, contempt, or ridicule. However, while cyberbullying can occur through both direct,

private electronic communications and public digital spaces, civil defamation strictly requires proof of publication, meaning the defamatory statement must be communicated to a third party beyond the victim.

The application of civil defamation principles to online harassment is illustrated in *Masyitah binti Md Hassan v. Sakinah binti Sulong* [2021] 7 MLJ 144. In this case, the court ruled in favor of the plaintiff after the defendant initiated a targeted online campaign, published derogatory Facebook posts, and responded maliciously to public comments, thereby exposing the plaintiff to online character assassination. This decision highlights how public online accusations that damage reputation can constitute cyberbullying and form the basis of a civil defamation action. Nevertheless, because the Defamation Act 1957 provides only civil remedies rather than criminal sanctions, plaintiffs must establish three core common law elements: that the statement is defamatory, that it refers to the plaintiff, and that it was published to a third party.²⁴

5) *Evidence Act 1950*

Although not specifically enacted for digital harassment, the Evidence Act 1950 impacts cyberbullying litigation through Section 114A. This provision establishes a statutory presumption that online content published under a person's name, image, or registered network/device originates from that individual. By shifting the burden of proof onto the defendant²⁵ to disprove authorship—as illustrated in *Thong King Chai v. Ho Khar Fun* [2018] 1 LNS 374—Section 114A assists in identifying anonymous bullies. However, it remains contentious because it exposes victims of hacking, identity theft, or open Wi-Fi misuse to vicarious liability. Consequently, Section 114A highlights an ongoing tension between facilitating digital law enforcement and protecting innocent parties from unjust liability.

Psychological Effects of Cyberbullying Against the Athletes

Primary empirical data gathered from semi-structured interviews with 16 elite Malaysian athletes reveals three major qualitative impact dimensions: emotional trauma, mental health deterioration, and career disruption. The first empirical theme derived from the qualitative interview data captures the emotional impact of cyberbullying on athletes, defined as the adverse affective reactions triggered by targeted digital harassment. It was hypothesized that online abuse causes acute emotional distress, thereby impairing an athlete's psychological state and daily focus across both personal and professional domains. In line with this expectation, participants detailed pervasive experiences of distress, frustration, and psychological harm stemming from hostile online commentary and coordinated cyber-attacks.

²⁴ Lisa Ward and Julia Day, “Defamation and Social Media Law,” in *Research Handbook on Social Media and the Law* (Edward Elgar Publishing, 2025), 8–37, <https://doi.org/10.4337/9781035309498.00007>.

²⁵ Olivia K. H. Smith, “The beyond a Reasonable Doubt Standard of Proof: Juror Understanding and Reform,” *The International Journal of Evidence & Proof* 26, no. 4 (October 2022): 291–308, <https://doi.org/10.1177/13657127221114498>.

Table 2. Empirical Interview Data on the Emotional Impact of Cyberbullying on Athletes

Respondent	Theme / Sub-theme	Emotional Impact (Direct Quote)	Analytical & Behavioral Insight
Respondent 5	Targeted Harassment & Personal Safety Concerns	“It was kind of like targeted harassment, because he used to undermine my performances online and give constant negative comments, but then I felt threatened that I would bump into him in real life, and I actually did.” “It was threatening my safety.”	Illustrates how online targeted harassment can escalate into perceived real-world threats, producing genuine apprehension about personal safety and prompting avoidance behaviors.
Respondent 12	Performance Distraction & Loss of Confidence	“Before, during, and after competition, normally I don’t open social media because when I see those comments, it makes me feel bothered and will disturb my confidence, so I only open my Facebook and Instagram a few days after the competition ends.” “One time I read the comment before going to the competition and they commented on my strategy, so I was worried about using my usual method because I was scared that we might lose.”	Demonstrates how hostile public commentary disrupts focus and self-efficacy, leading athletes to avoid social media around competitions and alter strategies due to diminished confidence.
Respondent 16	Powerlessness & Suppressed Frustration	“Sometimes I get angry and irritated when I see those comments, but I feel powerless because confronting them will only cause more problems.”	Highlights learned helplessness and psychological distress; athletes suppress negative emotions to avoid escalation, which may exacerbate internalized stress.

Source: Compiled by the author based on the results of interviews conducted via the Zoom platform

The second theme derived from the qualitative interview data examines the impact of cyberbullying on athletes’ mental health, focusing on how sustained online harassment impairs cognitive, emotional, and behavioral functioning. Grounded in the hypothesis that chronic digital abuse severely erodes psychological resilience and overall well-being, this theme explores the long-term mental health toll experienced by elite competitors. As anticipated, participant testimonies detailed acute psychological distress, heightened anxiety, and burnout resulting from relentless online hostility.

Table 3. Empirical Interview Data on the Mental Health Impact of Cyberbullying on Athletes

Respondent	Sub-Theme	Mental Health Impact (Direct Quote)	Behavioral & Analytical Insight
Respondent 7	Performance Anxiety & Fear of Reprisal	“I have anxieties because I’m worried I might bump into my bully and he will throw hate comments about my performance on me.” “It is very pressuring for us to take even one shot, because if we miss it, they will blame us, so we will be nervous to even take a shot.”	Illustrates severe performance anxiety and hyper-vigilance, where public online harassment directly interferes with real-time athletic execution and decision-making under pressure.
Respondent 14	Impaired Self-Efficacy & Cognitive Self-Doubt	“I will doubt myself whether what I’m doing now is correct or not, because I’m worried that he will comment about my performance.” “That is where we start questioning ourselves about what we did wrong and where it went wrong.”	Demonstrates how persistent digital toxicity internalizes into debilitating self-doubt, eroding professional confidence and cognitive self-efficacy.
Respondent 15	Social Withdrawal & Depressive Symptoms	“For a certain period of time, I didn’t want to talk to people.”	Highlights acute social withdrawal and isolation as a psychological coping mechanism in response to targeted online abuse.

Source: Compiled by the author based on the results of interviews conducted via the Zoom platform

The third qualitative theme examines the professional impact of cyberbullying, defined as the degree to which online abuse impairs an athlete's career trajectory, competitive performance, commercial opportunities, and public reputation. This dimension captures operational disruptions such as compromised competitive focus during major tournaments, strained team cohesion, and diminished fan engagement. Grounded in the hypothesis that targeted digital harassment substantially hinders professional advancement and athletic execution, this theme evaluates qualitative testimonies detailing how online hostility induces performance distractions during training and live competition.

Table 4: Empirical Interview Data on the Professional Impact of Cyberbullying on Athletes

Respondent	Qualitative Sub-Theme	Professional Impact Described (Direct Quote)	Behavioral & Analytical Insight
Respondent 9	Disruption of Team Dynamics & Interpersonal Friction	“It creates a chaotic situation on the team, like, why do people like her more than they like me. So when there are such questions, sometimes there is jealousy between the	Demonstrates how online fan toxicity and targeted favoritism fracture team cohesion, replacing collective tactical cooperation with interpersonal rivalry and

Respondent	Qualitative Sub-Theme	Professional Impact Described (Direct Quote)	Behavioral & Analytical Insight
		players so rather than playing for the team, they will focus on increasing their performance only.”	insular performance behaviors.
		“It creates tension between the players.”	
Respondent 10	Career Abandonment & Travel Safety Concerns	“Of course, I am very worried. If you ask me to go to the Philippines also I will be very worried for my own safety.” “When I experienced it I actually wanted to stop playing because mentally I couldn't get myself to complete even one tournament.”	Highlights how intense cyber-harassment leads to genuine fears for physical safety during international competitions, ultimately driving high-level athletes toward premature career abandonment and psychological burnout.
Respondent 13	Media Avoidance & Brand Detachment	“I avoided the media as much because I didn't want to face criticism.”	Illustrates professional withdrawal as a defensive coping strategy, where athletes deliberately avoid public engagements and media interactions, potentially damaging their public relations and commercial sponsorship

Source: *Compiled by the author based on the results of interviews conducted via the Zoom platform*

The qualitative data in Table 9 outlines the empirical findings regarding the mental health impacts of cyberbullying on elite athletes. The thematic analysis reveals that sustained online harassment extends beyond momentary distress, manifesting in performance anxiety, impaired self-efficacy, and severe social withdrawal. These testimonies illustrate how public digital toxicity directly compromises athletes' cognitive focus, emotional resilience, and overall psychological well-being in competitive environments.

Table 5. Empirical Qualitative Analysis of the Mental Health Impact of Cyberbullying on Athletes

Respondent	Qualitative Sub-Theme	Mental Health Impact Described (Direct Quote)	Behavioral, Psychological & Analytical Insight
Respondent 7	Performance Anxiety & Fear of Reprisal	“I have anxieties because I’m worried I might bump into my bully and he will throw hate comments about my performance on me.” “It is very pressuring for us to take even one shot, because if we miss it, they will blame us, so we will be nervous to even take a shot.”	Illustrates hyper-vigilance and acute performance anxiety, where chronic online harassment impairs fine motor control, confidence, and live decision-making during competition.
Respondent 14	Impaired Self-Efficacy & Cognitive Self-Doubt	“I will doubt myself whether what I’m doing now is correct or not, because I’m worried that he will comment about my performance.” “That is where we start questioning ourselves about what we did wrong and where it went wrong.”	Demonstrates how persistent digital toxicity internalizes into debilitating self-doubt, eroding internal self-efficacy and driving intrusive cognitive rumination.
Respondent 15	Social Withdrawal & Depressive Symptoms	“For a certain period of time, I didn’t want to talk to people.”	Highlights acute interpersonal withdrawal and social isolation as a protective coping mechanism in response to severe public online shaming.

Source: *Compiled by the author based on the results of interviews conducted via the Zoom platform*

Qualitative interviews with sixteen elite athletes across diverse sporting disciplines revealed several recurrent empirical themes emphasizing the profound mental and emotional distress resulting from cyber-victimization. The findings demonstrate that digital harassment directly impairs athletes' self-confidence, identity, social relationships, and competitive performance. Participant testimonies confirm that the relentless, boundaryless nature of online abuse undermines tactical concentration, damages public reputation, and compels athletes to withdraw from public interactions to preserve their mental health. Collectively, these empirical insights underscore the acute vulnerabilities faced by sports professionals and highlight the urgent imperative for robust legal and institutional protective frameworks in Malaysia.

The Strengths of Malaysia's Existing Governing Laws

Without a dedicated standalone statute, Malaysia addresses digital harassment through a fragmented framework of legacy statutes.²⁶ These include the Communications and Multimedia Act (CMA) 1998, the Penal Code (Act 574), the Minor Offenses Act 1955, the Defamation Act 1957, and the Evidence Act 1950. Together, these statutory provisions provide mechanisms to hold cyberbullies accountable across various criminal and civil dimensions depending on the nature of the misconduct.

A primary statutory mechanism within this matrix is Section 233 of the CMA 1998, which penalizes the improper use of network facilities or application services. Section 233(1)(a) criminalizes making, creating, soliciting, or initiating the transmission of comments or communications that are obscene, indecent, false, menacing, or grossly offensive with the intent to annoy, abuse, threaten, or harass another person. Offenders face severe punitive sanctions, including fines up to RM500,000, imprisonment for up to two years, or both, alongside a daily continuing fine of RM5,000 post-conviction. These substantial financial and custodial penalties serve both retributive and general deterrent functions.

To address the challenge of digital anonymity, Section 114A of the Evidence Act 1950 creates a statutory presumption of publication.²⁷ This provision presumes that any electronic content published from a specific IP address, mobile device, or registered account originated from the owner or administrator, shifting the burden of proof onto the defendant to disprove authorship (*Thong King Chai v. Ho Khar Fun* [2018] 1 LNS 374). Complementing these enactments, the Penal Code provides criminal sanctions against intimidation and privacy invasions. Section 503 penalizes criminal intimidation, while Section 509 targets gestures or words intended to insult modesty or intrude upon privacy. Furthermore, Section 507A (enacted in 2023) criminalizes repeated physical or online stalking causing fear, alarm, or distress, carrying a maximum sentence of three years' imprisonment.

In civil jurisprudence, the Defamation Act 1957 allows victims to pursue damages and injunctive relief for reputational harm. Under Section 3, electronic broadcasts are treated as permanent libel (*actionable per se*), bypassing the requirement to prove special financial damage. *Masyitah binti Md Hassan v. Sakinah binti Sulong* [2021] 7 MLJ 144 demonstrated the efficacy of civil defamation in addressing targeted digital smear campaigns, where the court held the defendant liable for publishing defamatory Facebook posts and orchestrating online hostility. Judicial precedents such as *PP v. Rutinin Subaimin* [2014] 5 MLJ 282 and *Mohd Fahmi Reza v. PP* [2020] 7 MLJ 399 further confirm the judiciary's willingness to enforce Section

²⁶ "Assessing Legal Protections against Cyberstalking: A Comparative Analysis of Malaysia, Singapore, Indonesia, and India," *Akademika* 96, no. 01 (April 2026), <https://doi.org/10.17576/akad-2026-9601-04>.

²⁷ Daniel Seng, "Artificial Intelligence as Evidence," in *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing, 2025), 373–401, <https://doi.org/10.4337/9781035316496.00026>.

233 of the CMA 1998 against online abuse.

Recent statutory updates, including proposed amendments under the Communications and Multimedia (Amendment) Bill to escalate penalties for offenses against minors, reflect legislative responsiveness. Concurrently, civil society engagement with international human rights benchmarks, such as Article 19 of the Universal Declaration of Human Rights 1948 (UDHR), promotes an equitable balance between mitigating digital harm and protecting individual expression and online privacy.²⁸

Systemic Weaknesses and Enforcement Challenges

Despite these statutory strengths, Malaysia's reliance on general enactments creates structural vulnerabilities and enforcement bottlenecks. Chief among these challenges is the absence of a unified, standalone anti-cyberbullying statute codifying explicit statutory definitions and key constituent elements (*actus reus* and *mens rea*).

Section 233 of the CMA 1998 remains highly contentious due to the textual ambiguity of subjective terms like 'grossly offensive' and 'intent to annoy'.²⁹ This vagueness invites judicial inconsistency and sparks concerns regarding potential overreach that could infringe upon the fundamental right to freedom of speech and expression guaranteed under Article 10(1)(a) of the Federal Constitution. Furthermore, legacy provisions within the Penal Code lack modern technological context.³⁰ Section 503 was originally enacted to regulate physical criminal intimidation and struggles to address non-physical digital harassment modalities such as doxxing, impersonation, or algorithmic swarming. Similarly, criminal defamation under Section 499 requires a high standard of proof and fails to account for the rapid, viral dissemination of malicious content on social media.

A critical enforcement gap exists under Section 14 of the Minor Offenses Act 1955. Because prosecutors lack a dedicated cyberbullying offense, Section 14 is frequently utilized as a fallback charge for online trolling. However, its statutory maximum penalty of merely RM100 is manifestly inadequate, failing to deliver retribution or general deterrence, a defect highlighted in the tragic 2024 suicide of TikTok influencer Esha (Rajeswary Appahu). To resolve statutory fragmentation, Malaysia should execute a dual-track reform strategy: enacting a dedicated standalone Anti-Cyberbullying Act alongside parallel modernizations of existing legacy statutes.

The proposed legislation would serve as the primary *lex specialis* for digital abuse,

²⁸ Francois Regis Nshimiyimana, "Balancing Cybersecurity and Fundamental Rights: The Responsibility of States to Address Cyber Threats," *Essays of Faculty of Law University of Pécs, Yearbook of [Year]*, no. 1 (June 2025), <https://doi.org/10.15170/studia.2025.01.15>.

²⁹ Siti Zaharah Jamaluddin, Mohammad Abu Taher, and Iman Syamil Ahmad Rujhan, "Sharenting in Malaysia: Balancing Parental Rights and Children's Privacy in the Digital Age," *Hasanuddin Law Review*, July 2025, 161–82, <https://doi.org/10.20956/halrev.v11i2.6285>.

³⁰ S. El-Manaseer et al., "Technological Impact on the Evolution of Sentencing Practices in the Criminal Justice System: A Critical Analysis of Recent Legal Changes," 2025, 973–84, https://doi.org/10.1007/978-3-031-87584-7_70.

featuring:

- a) Clear statutory definitions for modern modalities of abuse, including cyberbullying, doxxing, online impersonation, and digital swarming, alongside codified *actus reus* (non-consensual digital communications) and *mens rea* (intent to cause distress or reasonable apprehension of harm).
- b) Proportional penalties ranging from community service and mandatory cyber-ethics education for minor first-time offenders to custodial terms for recidivists. The framework must align with the Child Act 2001 by establishing age-specific statutory pathways and rehabilitative programs.
- c) Fast-tracked civil remedies such as emergency digital restraining orders enabling sports governing bodies (KBS, MSN, OCM) to secure immediate injunctive relief during high-stakes tournaments.
- d) Clear statutory parameters preventing recourse to trivial fines under Section 14 of the Minor Offenses Act 1955, while prioritizing immediate administrative takedown orders to protect victims prior to trial conclusions.

In Parallel to the existing legislation, this research proposed:

- a) To insert in the CMA Section 233 statutory explanatory notes and concrete illustrative examples (e.g., doxxing, deepfake pornography) to eliminate textual ambiguity and safeguard constitutional speech under Article 10(1)(a).
- b) To expand Section 503 of the Penal Code to cover persistent, encrypted messaging threats and model Section 507A after international comparative frameworks to recognize cyber-stalking as an autonomous crime.
- c) To introduce statutory safe-harbor clauses in section 114A of the Evidence Act 1950 to protect victims of account hacking, open Wi-Fi network hosts, and system administrators from unjust reverse-burden prosecutions.

Conclusion

This study demonstrates that Malaysia's current approach to addressing cyberbullying, which relies primarily on a fragmented application of general legislation such as the Communications and Multimedia Act 1998, Penal Code, Minor Offenses Act 1955, Defamation Act 1957, and Evidence Act 1950, presents significant limitations in responding effectively to the evolving nature of digital harassment. The doctrinal analysis reveals that these existing legal frameworks were not specifically designed to regulate cyberbullying and therefore lack a comprehensive statutory definition, clearly established constituent elements (*actus reus* and *mens rea*), and tailored procedural mechanisms for addressing online abuse. These limitations create uncertainty in enforcement and may limit timely, effective remedies for victims. This concern is particularly evident in cases involving minor offenses, where the relatively low penalty under section 14 of the Minor Offenses Act 1955 has raised questions regarding the adequacy and deterrent effect of existing legal responses.

The empirical findings from qualitative interviews with 16 national athletes further demonstrate the practical consequences of these legal limitations. The participants reported that performance-related cyberbullying and digital hostility generated significant emotional distress, including anxiety, reduced confidence, interpersonal tension within teams, and, in some cases, considerations of withdrawing from competitive sports. These findings illustrate that cyberbullying extends beyond reputational harm and may produce substantial psychological and professional consequences, particularly for public figures whose identities and performances are constantly exposed in digital spaces.

The implications of this study are twofold. First, the continued reliance on conventional legal provisions developed for offline misconduct creates challenges in regulating cyberbullying within a borderless, rapidly disseminating, and technologically complex environment. The absence of a dedicated legislative framework may lead to inconsistent enforcement, difficulty establishing liability, and inadequate access to timely remedies for victims. Second, unclear and broadly framed legal provisions may raise concerns regarding proportionality and constitutional balance, particularly in relation to Article 10(1)(a) of the Federal Constitution, which guarantees freedom of speech and expression. Any regulatory response must therefore ensure that restrictions on online expression are sufficiently precise, necessary, and proportionate.

In addressing these challenges, this study supports growing scholarly and policy recommendations to strengthen Malaysia's cyberbullying governance framework. Rather than relying solely on piecemeal amendments, Malaysia should consider developing a more coherent legislative approach through either substantial reform of existing laws or the introduction of a dedicated Anti-Cyberbullying Act. Such legislation should provide a clear statutory definition of cyberbullying, establish objective legal elements for liability, introduce victim-centered protection mechanisms, and clarify the responsibilities of relevant enforcement authorities and digital platforms. Procedural safeguards, including accessible reporting mechanisms, timely intervention measures, and proportionate penalties, are essential to ensure effective protection without undermining legitimate freedom of expression. Ultimately, Malaysia requires a balanced regulatory framework that recognizes the serious harms caused by cyberbullying while preserving constitutional principles. A purpose-built legal regime, guided by proportionality, due process, and human rights standards, would enable Malaysia to respond more effectively to digital harassment and provide meaningful protection for vulnerable groups, including athletes and other public figures exposed to heightened online scrutiny.

Acknowledgement

The authors would like to express their sincere appreciation to all individuals and entities who provided essential support in completing this study. We are particularly grateful to the athletes who generously contributed their time, experiences, and insights as research participants.

References

- Abdul Raof, Nurazlina, Norazlina Abdul Aziz, Nadia Omar, Rozita Othman, and Hasiah Mat Salleh. "Exploring the Depths: A Comparative Analysis of Doctrinal and Non-Doctrinal Legal Research." *International Journal of Research in Social Science and Humanities* 06, no. 05 (2025): 122–29. <https://doi.org/10.47505/IJRSS.2025.5.13>.
- "Assessing Legal Protections against Cyberstalking: A Comparative Analysis of Malaysia, Singapore, Indonesia, and India." *Akademika* 96, no. 01 (April 2026). <https://doi.org/10.17576/akad-2026-9601-04>.
- Basu, Subhajit, and Shameek Sen. "Silenced Voices: Unravelling India's Dissent Crisis through Historical and Contemporary Analysis of Free Speech and Suppression." *Information & Communications Technology Law* 33, no. 1 (January 2024): 42–65. <https://doi.org/10.1080/13600834.2023.2249780>.
- Bosher, Hayleigh. "Do Deepfakes, Digital Replicas and Human Digital Twins Justify Personality Rights?" *The Journal of World Intellectual Property*, March 2026. <https://doi.org/10.1111/jwip.70020>.
- Dixon, Kevin. "Content Leakage: Privacy, Exposure and the Athlete in the Public Eye." In *Combating Online Abuse in Sports*, 37–63. Cham: Springer Nature Switzerland, 2026. https://doi.org/10.1007/978-3-032-17822-0_3.
- EI-Manaseer, S., Omar Almakhoum, Ali Awwad Aljabrah, and Jalal Hussein Hamdan Alkayid. "Technological Impact on the Evolution of Sentencing Practices in the Criminal Justice System: A Critical Analysis of Recent Legal Changes," 973–84, 2025. https://doi.org/10.1007/978-3-031-87584-7_70.
- Gautam, Sanskriti. "Freedom of Speech and Expression: Responses to Online Harassment," 2025. <https://doi.org/10.2139/ssrn.5210246>.
- Goyanes, Manuel, Carlos Lopezosa, and Beatriz Jordá. "Thematic Analysis of Interview Data with ChatGPT: Designing and Testing a Reliable Research Protocol for Qualitative Research." *Quality & Quantity* 59, no. 6 (December 2025): 5491–5510. <https://doi.org/10.1007/s11135-025-02199-3>.
- Hennink, Monique, and Bonnie N. Kaiser. "Sample Sizes for Saturation in Qualitative Research: A Systematic Review of Empirical Tests." *Social Science & Medicine* 292 (January 2022): 114523. <https://doi.org/10.1016/j.socscimed.2021.114523>.
- Jamaluddin, Siti Zaharah, Mohammad Abu Taher, and Iman Syamil Ahmad Rujhan. "Sharenting in Malaysia: Balancing Parental Rights and Children's Privacy in the Digital Age." *Hasanuddin Law Review*, July 2025, 161–82. <https://doi.org/10.20956/halrev.v11i2.6285>.
- Kim, Sangmi, Seon-Kyeong Ahn, Eunbyeor Sophie Yang, Seohyun Kim, and Ick-Joong Chung. "The Evolution of Cyberbullying Definitions in the Digital Age:

- A Systematic Review of Defining Attributes and Conceptual Synthesis.” *Journal of Technology in Human Services*, March 2026, 1–31. <https://doi.org/10.1080/15228835.2026.2647023>.
- Lim, Weng Marc. “What Is Qualitative Research? An Overview and Guidelines.” *Australasian Marketing Journal* 33, no. 2 (May 2025): 199–229. <https://doi.org/10.1177/14413582241264619>.
- Lim, Willone, Bee Theng Lau, Swee Tee Fu, Mark Kit Tsun Tee, and Fakir M. Amirul Islam. “Sociodemographic Factors Associated with Cyberbullying Experience and Practice Among Youths in Malaysia.” *Journal of Technology in Behavioral Science* 10, no. 3 (December 2024): 613–23. <https://doi.org/10.1007/s41347-024-00469-9>.
- Majeed, Nasir, Amjad Hilal, and Arshad Nawaz Khan. “Doctrinal Research in Law: Meaning, Scope and Methodology.” *Bulletin of Business and Economics (BBE)* 12, no. 4 (December 2023): 559–63. <https://doi.org/10.61506/01.00167>.
- Mishna, Faye, Arija Birze, and Andrea Greenblatt. “Understanding Bullying and Cyberbullying Through an Ecological Systems Framework: The Value of Qualitative Interviewing in a Mixed Methods Approach.” *International Journal of Bullying Prevention* 4, no. 3 (September 2022): 220–29. <https://doi.org/10.1007/s42380-022-00126-w>.
- Nikiforov, Liubomir. “The Law Enforcement Directive 2016/680 in Practice: Transparency, Lawfulness and Strict Necessity. Lessons from Bulgaria.” *Computer Law & Security Review* 62 (September 2026): 106370. <https://doi.org/10.1016/j.clsr.2026.106370>.
- Njeri Mugwe, Jayne, and Steven Runo. “Qualitative Data Analysis.” In *Research Methodology in Agricultural Sciences*, 561–83. Singapore: Springer Nature Singapore, 2026. https://doi.org/10.1007/978-981-95-1892-0_23.
- Nshimiyimana, Francois Regis. “Balancing Cybersecurity and Fundamental Rights: The Responsibility of States to Address Cyber Threats.” *Essays of Faculty of Law University of Pécs, Yearbook of [Year]*, no. 1 (June 2025). <https://doi.org/10.15170/studia.2025.01.15>.
- O’Higgins Norman, James, Christian Berger, Shoko Yoneyama, and Donna Cross. “School Bullying: Moving beyond a Single School Response to a Whole Education Approach.” *Pastoral Care in Education* 40, no. 3 (July 2022): 328–41. <https://doi.org/10.1080/02643944.2022.2095419>.
- Philipo, Adamu Gaston, Doreen Sebastian Sarwatt, Jianguo Ding, Mahmoud Daneshmand, and Huansheng Ning. “Cyberbullying Detection: Exploring Datasets, Technologies, and Approaches on Social Media Platforms.” *ACM Computing Surveys* 58, no. 7 (May 2026): 1–35. <https://doi.org/10.1145/3785654>.
- Rakymbaeva, Meruert, Arstan Akhpanov, Bakitkul Sembekova, Aydarkan Skakov,

- Yerbol Karzhaubayev, and Dinara Osmanova. “Cyberbullying of Minors and Juvenile Justice: Digital Evidence and Chain-of-custody in Suicide Incitement Cases.” *Juvenile & Family Court Journal*, July 2026. <https://doi.org/10.1111/jfcj.70031>.
- Santos, Isadora Mendes Dos, Ronald Pinto Marques, Vinicius Augusto Carvalho de Abreu, and Marcelle Pereira Mota. “Social Media for Whom? The Absence of Guideline Adherence in Social Platforms.” *IEEE Access* 14 (2026): 53360–77. <https://doi.org/10.1109/ACCESS.2026.3680543>.
- Sarmini. “From Memes to Harassment Automated Detection of Cyberbullying for Cyberlaw Enforcement.” *Journal of Cyber Law* 1, no. 4 (December 2025). <https://doi.org/10.63913/jcl.v1i4.3>.
- Seng, Daniel. “Artificial Intelligence as Evidence.” In *Research Handbook on the Law of Artificial Intelligence*, 373–401. Edward Elgar Publishing, 2025. <https://doi.org/10.4337/9781035316496.00026>.
- Smith, Olivia K. H. “The beyond a Reasonable Doubt Standard of Proof: Juror Understanding and Reform.” *The International Journal of Evidence & Proof* 26, no. 4 (October 2022): 291–308. <https://doi.org/10.1177/13657127221114498>.
- Tod, David, Samuel Pullinger, and Moira Lafferty. “A Systematic Review of the Qualitative Research Examining Stakeholders’ Perceptions of the Characteristics of Helpful Sport and Exercise Psychology Practitioners.” *International Review of Sport and Exercise Psychology* 17, no. 2 (December 2024): 1312–36. <https://doi.org/10.1080/1750984X.2022.2145575>.
- Ward, Lisa, and Julia Day. “Defamation and Social Media Law.” In *Research Handbook on Social Media and the Law*, 8–37. Edward Elgar Publishing, 2025. <https://doi.org/10.4337/9781035309498.00007>.
- Yanis, Tryan Zaki Aulia, Muhtadi, Ahmad Saleh, and Adam M. Yanis. “The Unconstitutionality of the Offence of Insulting the Government in the 2023 Criminal Code: A Critical Review of Freedom of Expression.” *As-Siyasi: Journal of Constitutional Law* 5, no. 1 (June 2025): 111–19. <https://doi.org/10.24042/as-siyasi.v5i1.24739>.
- Ying Bong, Jasmeen Kah, Kasturi Dewi Varathan (Corresponding Author), and Teoh Hwai Teng. “Cyberbullying Detection In Social Media Using Pre-Trained Language Models.” *Malaysian Journal of Computer Science* 38, no. 1 (December 2025): 29–54. <https://doi.org/10.22452/mjcs.vol38no1.2>.