Introduction

The prevalence of cyberbullying and cyber-attacks has become a pressing concern globally. With Malaysia's burgeoning digital landscape, the tech-savvy population is not immune to these challenges. This comes into concern where digital platforms serve as both playgrounds and battlegrounds. From malicious online harassment campaigns to sophisticated cyber intrusions, the realm of cyberspace presents a complex legal frontier that demands scrutiny and robust legal frameworks.

This article explores the legal landscape governing cyberbullying and cyber-attacks in Malaysia, including key legislative measures, notable case studies, and the proposed changes that have been made thus far in Malaysia's evolving cyber legal framework.

Cyber-attacks in Malaysia

Cybercriminals target a wide range of victims, from individuals to companies and government agencies.[1] In 2023, Kaspersky reported blocking 26.85 million "internet-borne" attacks in Malaysia, an estimated figure of 74,000 attacks daily.[2] PwC's 2023 Global Risk Survey found 69% of organizations view themselves as highly exposed to cyber risks.[3]

Cyber-attacks, including malware, ransomware, phishing, and more can cause unauthorized access, business disruptions, and data breaches, leading to financial losses and reputational damage.[4]

A global survey shows that 40% of respondents would cease doing business with a company that has experienced a data breach involving personally identifiable information or sensitive financial information.[5]

Cyberbullying in Malaysia

In 2023, the Malaysian Communications and Multimedia Commission ("**MCMC**") recorded 3,199 cyberbullying complaints involving bullying, intimidation, and misuse of personal information across platforms like TikTok, Facebook, and Instagram.[6] Dr Rozanizam Zakaria of the International Islamic University Malaysia notes that persistent cyberbullying poses a higher risk of suicidal thoughts and behaviour compared to traditional bullying.

Key Legislative Measures

Cyber-attacks

Currently, there is no specific legislation in Malaysia that exclusively regulates cyber-attacks or cyberbullying. Instead, these issues are addressed under existing laws including the Computer Crimes Act 1997, the Personal Data Protection Act 2010, and the Penal Code.

(a) Computer Crimes Act 1997 ("**CCA**")

Under Section 3 of the CCA, having an unauthorised access to computer data amounts to an offense.[7] If such unauthorized access is aimed to commit fraud or harm someone, it constitutes an offence under Section 4.[8] Additionally, Section 5 stipulates that it is an offence to knowingly alter another computer's data without authorization.[9] The CCA restricts the definition of "computer" to physical devices that perform logical, arithmetic, storage, and display functions.[10]

(b) Personal Data Protection Act 2010 ("**PDPA**")

While CCA penalises the cybercriminals for unauthorised access, the PDPA requires data users such as corporations and organisations to protect personal data from unauthorised access, modification, destruction and use.[11] Under Sections 5 and 9 of the PDPA, corporations may face criminal liability for not adhering to security principles and failing to implement reasonable security measures to safeguard personal data, as highlighted by Malaysian legal precedents.[12]

(c) Penal Code

Despite the significant increase in online identity theft and fraud in Malaysia, there are no specific laws addressing these issues. Some suggest Section 416 of the Penal Code which criminalises "cheat by personation", might apply as it covers deceiving others by pretending to be someone else.[13] Offenders can face up to seven years in prison and/or a fine.[14] However, there have been no cases to date applying this section to online fraud, raising doubts about its effectiveness in tackling such crimes.

Cyberbullying

The absence of a specific legal framework in Malaysia for addressing cyberbullying has created a gap in effectively tackling this growing concern. While there are no dedicated laws solely targeting cyberbullying, existing legislation provides mechanisms to hold individuals accountable for their actions. Relevant laws include the Communication and Multimedia Act 1998, the Penal Code, the Defamation Act 1957, the Minor Offences Act, and the Evidence Act 1950.

(a) Communication and Multimedia Act 1998 ("**CMA**")

While the CMA does not explicitly address cyberbullying as a criminal offence, it targets behaviours like obscenity, indecency, and threat.[15] Key considerations include (i) whether the communication is classified as 'content',[16] (ii) whether the transmission of the 'content' constitutes a form of 'communication'[17] through an 'application service'[18] and (iii) if it was intended to annoy or harass.[19] If an individual knowingly fulfils all of these conditions, they may be found to have committed an improper use of network facilities or network services.[20] The Content Code outlines what is considered obscene, indecent, false, menacing, or offensive to prevent online bullying and maintain a safe digital environment.[21] The provisions under the CMA offer a framework for addressing instances of cyberbullying by targeting online content or communication that falls within the parameters mentioned.

(b) Penal Code

The Penal Code includes threats in cyberbullying as criminal intimidation, particularly if the threats involve death, grievous hurt, destruction of property, or attributing unchastity to a woman.[22] Anonymity often deters victims from reporting the offence, but with technological advancement, the tracking and identification of user identities allows the Prosecution to prove that criminal intimidation was present.[23]

(c) Defamation Act 1957

Given the broad nature of cyberbullying, it is also relevant to assess it under defamation law. According to the High Court, the determination of whether words are defamatory is dependent on how a reasonable person interprets them in context.[24] To prove defamation, three elements must be satisfied: (i) the statement is defamatory, (ii) it is targeted on an individual, and (iii) it is published.[25] The Honourable Judge Gopal Sri Ram emphasized that the court's role is to determine if the words have a defamatory meaning.[26] The Defamation Act 1957 underpins many defamation claims related to cyberbullying, encompassing both libel and slander.[27]

(d) Minor Offences Act 1955

If cyberbullying cannot be proven under existing legal frameworks, the Minor Offences Act may serve as a last resort. For instance, in the case of Malaysian TikTok influencer,

Rajeswary Appahu, also known as Esha who was a victim of online harassment and cyberbullying,[28] the offender faced a maximum fine of RM100.[29] While some find these penalties too lenient for its consequences, [30] the Act still helps address the issue of cyberbullying.

(e) Evidence Act 1950

Section 114A of the Evidence Act 1950 holds service providers accountable for moderating user actions to combat cyberbullying.[31] The said Section presumes that: (i) a person's identity is linked to online content, (ii) the identity be associated to the publication as an owner or editor, and (iii) the service providers facilitated the content's publication unless proven otherwise.[32] An example of the application of the Evidence Act can be seen in the case of Malaysiakini's failure to filter offensive comments, the court fined them RM500,000,[33] highlighting the need for service providers to ensure safe and responsible platform management.

Proposed Changes in the Legal Framework

Cyber-Attacks

The current legislation on cyber-attacks addresses the obligations of cybercriminals and data users, but lacks clarity on the roles of service providers or data processors.[34] To close this gap, it is proposed that service providers be given clear legal obligations to manage and store data securely. This would protect both data users' contractual benefits and individuals' personal information.

Further, the Personal Data Protection (Amendment) Bill 2024,[35] passed on 16 July 2024 has made data retention and security principles from the PDPA binding on service providers.

Additionally, it is recommended that the definition of "computer" in the CCA be broadened to include equipment beyond traditional computers, similar to the approach in Singapore's Computer Misuse Act 1993.[36] This would ensure that cyber-attacks involving devices like proxy servers are covered under the CCA.

Cyberbullying

MCMC now requires social media and messaging services with over eight million registered users in Malaysia to obtain a Class A Application Service License under the CMA.[37] This mandate enforces anti-cyberbullying policies, including identity verification, establishing content moderation policies, submitting regular transparency reports, and ensuring accountability under current legislation.[38]

---

1. Malaysia Computer Emergency Response Team, 'MA-1046.032024: MyCERT Advisory - Recent Increase in Cyber Attacks Targeting Malaysia' Advisories (19 March 2024) https://www.mycert.org.my/portal/advisory?id=MA-1046.032024.
2. 'Threat of cyber-attacks to remain on the rise in Malaysia this year' Bernama (Petaling Jaya, 20 February 2024) https://www.nst.com.my/lifestyle/bots/2024/02/1015562/threatcyber-attacks-remain-rise-malaysia-year.
3. 'Cyber and digital technology risks are a key concern for businesses and risk leaders, even as 60% see GenAI as an opportunity: PwC 2023 Global Risk Survey' PwC (20 November 2023) https://www.pwc.com/gx/en/news-room/pressreleases/2023/cyber-and-digital-technology-risks-are-akey-concern-for-businesses-and-risk-leaders.html.
4. 'One in four companies globally have suffered a data breach that cost them US$1 - 20 million or more in the past three years' PwC Press Release (29 September 2022) https://www.pwc.com/gx/en/news-room/press-releases/2022/global-digital-trust-insights-survey.html.
5. Internet Society, 'Global Internet Report 2016' page 58 https://www.internetsociety.org/wp-content/uploads/2022/12/2016-Internet-Society-Global-Internet-Report.pdf.
6. Qirana Nabilla Mohd Rashidi, "Over 3,000 Cyberbullying Complaints Recorded in 2023" The Sun (Petaling Jaya, 14 February 2024) https://thesun.my/local-news/over-3000-cyberbullying-complaints-recorded-in-2023-AK12097214.
7. Computer Crimes Act 1997, section 3.
8. Computer Crimes Act 1997, section 4; Penal Code, section 44.
9. Computer Crimes Act 1997, section 5.
10. Computer Crimes Act 1997, section 2.
11. Public Bank Bhd v Tan Teck Seng Jason & Anor [2021] MLJU 92 (HC) paragraph 19; Personal Data Protection Code of Practice, paragraph 4.5.
12. Public Bank Bhd v Tan Teck Seng Jason & Anor [2021] MLJU 92 (HC).
13. Penal Code, section 416; Wee, Richard & Low, May Ping "Identity Theft" Richard Wee Chambers (3 September 2020) https://www.richardweechambers.com/identity-theft/#:~:text=The%20offence%20is%20committed%20as,years%20and%2For%20a%20fine.
14. Penal Code, Section 416.
15. Communication and Multimedia Act 1998, section 233(1).
16. Communication and Multimedia Act 1998, section 6.
17. Communication and Multimedia Act 1998, section 6.
18. Communication and Multimedia Act 1998, section 6.
19. Communication and Multimedia Act 1998, section 233(1).
20. Communication and Multimedia Act 1998, section 6.
21. Guidelines on Content in the Malaysian Communications and Multimedia Content Code (Content Code) 2022, Part 2.
22. Penal Code, Section 503.
23. PP v Dato' Dr Ahmad Ramzi Ahmad Zubir [2015] 6 CLJ 1028 (COA) paragraph 35.
24. Dato' Musa bin Hitam v S.H Alattas & Ors [1991] 1 CLJ (Rep) 487 (HC).
25. Dato' Seri Mohammad Nizar Jamaluddin v Sistem Televisyen Malaysia Bhd & Anor [2014] 3 CLJ 560 (COA) paragraph 10; Ayob Saud v TS Sambanthamurthi [1989] 1 CLJ 152.
26. Chook Foo Choo @ Chok Kee Lian v The China Press Bhd [1999] 1 MLJ 371 (COA), page 374.
27. Razali, N. A., Nawang, N. I., & Mohamad, S. N. a. S. N., 'Cyberbullying in Malaysia: An Analysis of The Existing Laws' (2022) 7(30) International Journal of Law Government and Communication, page 131–132 https://doi.org/10.35631/ijlgc.730011?.
28. 'Cyberbullying: Two plead guilty to communications offences linked to Esha's death' The Star (Kuala Lumpur, 16 July 2024) https://www.thestar.com.my/news/nation/2024/07/16/cyberbullying-two-plead-guilty-to-communications-offences-linked-to-esha039s-death.

29. Minor Offences Act of 1955, section 14.
30. Anisah Shukry, 'TikTok user's death sparks Malaysia clampdown on cyberbullying' The Star (18 July 2024) https://www.thestar.com.my/tech/tech-news/2024/07/18/tiktok-users-death-sparks-malaysia-clampdown-on-cyberbullying.
31. Evidence Act 1950, Section 114A.
32. AG v Mkini Dotcom Sdn. Bhd. & Anor [2021] 3 CLJ 603 (FC), paragraph 135.
33. ibid. 158.
34. Computer Crimes Act 1997, sections 3, 4 and 5; Personal Data Protection Act 2010, sections 5 and 9; Penal Code, Section 416.
35. Personal Data Protection (Amendment) Bill 2024, clauses 2, 4, 5, 6, 8, and 12.
36. Computer Misuse Act 1993 (SG), Section 2.
37. Rahimy Rahim, 'Social media providers face fines, jail without valid licence by Jan 1, warns Fahmi' The Star (Putrajaya, 1 August 2024) https://www.thestar.com.my/news/nation/2024/08/01/social-media-providers-face-fines-jail-without-valid-licence-by-jan-1-warns-fahmi.
38. 'New licensing rules require social media providers to ensure safe online environment, says govt' The Star (Kuala Lumpur, 31 July 2024) https://www.thestar.com.my/news/nation/2024/07/31/new-licensing-rules-require-social-media-providers-to-ensure-safe-online-environment-says-govt.

Written by:

Natasha L Jayasinghe
general@azmilaw.com

Khong Ling Qi
Trainee Solicitor
khonglingqi@azmilaw.com

Maisarah Afifah Azunan
Trainee Solicitor
maisarah.azunan@azmilaw.com

Corporate Communications
Azmi & Associates
15 November 2024