

Joint Memorandum by the Online Safety Advocacy Group on the proposed Penal Code (Amendment) Bill & Online Safety Bill

PART 1: Responses on General Positions Taken & Policy Recommendations

Introduction

The Online Safety Advocacy Group comprises the following civil society organisations (CSOs) and individuals working on the issues of freedom of expression, child rights, gender equality, and women's rights:

- | | |
|---|--|
| 1. Centre for Independent Journalism (CIJ) | 10. Women's Centre for Change (WCC) |
| 2. Justice for Sisters | 11. Monsters Among Us (MAU) |
| 3. KRYSS Network | 12. Sarawak Women for Women Society (SWWS) |
| 4. Childline Foundation | 13. Association of Women Lawyers (AWL) |
| 5. Protect and Save the Children (PS The Children) | 14. Johor Women's League (JEWEL) |
| 6. End CSEC Network Malaysia (ECPAT Malaysia) | 15. Women's Aid Organisation (WAO) |
| 7. CRIB Foundation (Child Rights Innovation & Betterment) | 16. Sisters in Islam (SIS) |
| 8. Voice of the Children | 17. Sinar Project |
| 9. Kemban Kolektif | 18. Maha Balakrishnan |

Summary

This Memorandum is Part 1 of a collective two-part response from the Online Safety Advocacy Group regarding the government's proposed online safety and anti-cyberbullying laws ("Government's Proposals"). Our response is split into two parts as a result of the government's urgent request for our feedback on policy on or before 8 October 2024. As a result:

- (a) Part 1 of the Memorandum contains the Online Safety Advocacy Group's position on the policy rationale for the Government's Proposals and will be submitted to the government on 8 October 2024.
- (b) Part 2 of the Memorandum will contain detailed responses and counter-proposals to the government's specific provisions regarding ONSA and cyberbullying. The Part 2 Memorandum will be submitted shortly.

With regard to policy considerations, it is our collective position that the Government's Proposals as they stand are inadequate to alleviate our concerns on online safety and cyberbullying for the following reasons:

- (a) The government's stakeholder consultation process is incomplete and inadequate. A broader and more detailed stakeholder consultation process is required. We expand on this below.
- (b) It is neither necessary nor proportionate to create new anti-bullying laws in the Penal Code or otherwise. It is also not necessary, proportionate, or appropriate to insert new anti-cyberbullying laws or other online safety laws in the Penal Code.
- (c) Any online safety laws, including those relating to cyberbullying, should clearly distinguish between adults and children in terms of processes, procedures, safeguards, repercussions, and enforcement measures.
- (d) The enforcement of any online safety laws, including an Online Safety Act, could be best achieved with the setting up of an independent, specialised, multi-stakeholder regulatory body.

Responses

1. Lack of Consultation with Key Stakeholders

1.1 While the Law Minister and BHEUU have proactively engaged with certain stakeholders over the last 2 months, the process has been rushed, and many important groups and sectors were left out or under-represented.

1.2 In fact, our outreach to civil society and grassroots groups underscored to us that there is a critical need for further consultations with other key stakeholders and civil society groups, specifically those working on intersectional issues, including the rights of the child, women's rights and the rights of persons with disabilities. In addition, and to our best knowledge, there has not been any direct consultation - or any meaningful direct consultation - with children. These groups are often the most disproportionately harmed in online spaces and the least equipped with individual agency to respond.

1.3 A broad based consultation is critical to ensure that all insights and experiences inform the scope, parameters and systems which are appropriate and needed to address online harm.

1.4 Online harms are an ongoing threat to society and the economy. There may be an urgent need to find solutions, but any urgency cannot supersede the critical imperative to adequately consult all those who are most likely to be impacted by the consequences. We recommend that the tabling of the bills be delayed until further holistic and robust nationwide consultations are carried out with various stakeholders, including other civil society organisations, experts, and big tech.

2. Proposed Penal Code (Amendment) Bill

2.1 We are concerned that the proposed Penal Code (Amendment) Bill conflates offences of bullying and cyberbullying, as well as adults and children.

2.2 In order to create a new regulatory framework to monitor, prevent and sanction cyberbullying, it is neither necessary nor proportionate to create new anti-bullying laws in the Penal Code.

2.3 It is also not necessary, proportionate or appropriate to insert new anti-cyberbullying laws or other online safety laws in the Penal Code. Online safety laws including anti-cyberbullying laws should be in separate legislation. We provide our reasons below.

2.4 The provisions under the proposed bill are broad and encompass an overly wide spectrum of content and speech, making them open to arbitrary interpretation and abuse. This includes terms like alarm, abusive, insult, distress, and harassment, which fail to meet the test of legality, necessity, and proportionality -which are fundamental constitutional and legal principles.

2.5 The proposed criminal sanctions are disproportionate and do not address cases where the offender is a child below 18 years old. There is also no clarity on how the quantum of prison sentences has been determined.

2.6 Provisions on cyberbullying and online safety involving children should preferably be under separate legislation, which is harmonised with domestic laws such as the Child Act 2001, Sexual Offences Against Children Act 2017, Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007 (ATIPSOM), and other child protective legislation, and in line with international human rights law such as the Convention on the Rights of the Child (CRC) and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). Such legislation should focus on preventive measures and include non-punitive and rehabilitative approaches while upholding restorative and transformative justice for children.

2.6.1 Alternatively, provisions on cyberbullying in the proposed Online Safety Bill should clearly distinguish between adults and children regarding processes, procedures, safeguards, repercussions, and enforcement measures.

2.7 The Online Safety Advocacy Group is producing draft alternative legislative language for cyberbullying laws, to be submitted in Part 2 of this Memorandum shortly.

3. Regulation and Enforcement of Proposed Online Safety Bill (OSB)

3.1 The OSB should not be placed under the Minister / Ministry of Communications for the following reasons.

3.2 The Malaysian Communications and Multimedia Commission (MCMC) is not the appropriate regulatory body for the proposed OSB in terms of its current purpose, capacity, and composition for the following reasons:

3.2.1 The MCMC is not an independent regulatory body in law and practice. For instance, it can take (and has taken in the past) directives from the Minister in charge. This creates an opening for political or government interference, or selective prosecution, in cases that may carry political connotations and would ultimately put

users' speech under the control of a public authority with vast discretionary powers to determine what amounts to 'harmful' content. This could increase the risk of lawful content being taken down from the internet.

3.2.2 Additionally, the MCMC lacks the necessary expertise to deal with online safety. We have seen this in its current practice of blocking, censoring, and punishing users for their freedom of expression, leading to serious concerns about their ability to distinguish between freedom of expression (which includes criticism of politicians, public officials, and other public figures) and 'harmful' content.

3.2.3 What is required for the effective regulation, monitoring, and enforcement of online safety laws that will inspire public confidence is an independent and multi-stakeholder body that collectively has sufficient technical expertise and understanding of the equilibrium required in balancing freedom of expression, individual rights and safety, and community interests. Such an independent body must be legally vested with the necessary functions, power, and autonomy to regulate social media companies and service providers in Malaysia. The independent regulatory body should be empowered to administer accessible redress mechanisms. Part 2 of our Memorandum will contain a non-exhaustive list of qualifications, core functions, and powers of such a requisite regulatory body.

3.3 The protection of human rights should be at the centre of any regulation of social media companies and codified within the laws and regulations relating to online safety. This also means that at all stages of the enforcement process, the regulator should be legally required to ensure close involvement of civil society and independent experts with solid experience in these topics. Civil society organisations can provide evidence-based recommendations to the regulators and raise the voices of groups particularly impacted by the actions of online intermediaries.

4. 'Harmful' Content Covered under OSB

4.1 In relation to "kandungan memudaratkan" or 'harmful' content, we wish to highlight the following concerns:

4.1.1 *Kandungan 1 (Bahan penganiayaan seksual kanak-kanak)*

- (a) The definition of child sexual abuse material (CSAM) needs to be aligned with that in the Sexual Offences Against Children Act 2017. It should also include self-generated and AI-generated CSAM that can be taken and shared by children and young people as a result of online grooming or sextortion.
- (b) It is also important to balance these concerns against children's right to freely express themselves¹. In particular, self-generated sexual material by children that they possess and/or share with their consent and solely for their own private use should not be criminalized. Child-friendly channels should be created to allow children to safely seek advice and assistance where it relates to self-generated sexually explicit content.

¹ <https://inhope.org/EN/articles/what-is-self-generated-csa>

4.1.2 *Kandungan 2 (Kandungan seksual)*

- (a) The term 'sexual images' is too broad as it can also include images for educational, health-related, and awareness-raising purposes, where consent for the image or depiction was given on the basis that the image or depiction would be utilised within that specified purpose. A more precise definition is hence needed.
- (b) The focus should be on non-consensual intimate images (NCII) rather than sexual or intimate images per se.

4.1.3 *Kandungan 3 (Kandungan berkaitan dengan penipuan kewangan dalam talian)*

- (a) Content related to online scams should be dealt with separately, as it intersects with cybercrime and cybersecurity, which involve different regulatory authorities and require greater involvement with law enforcement in physical and digital spaces.
- (b) Measures to address online financial scams should consider UNODC's approach to online scams, and pull together safeguards, user empowerment measures, and education and training for enforcement and regulatory bodies.

4.1.4 *Kandungan 4 (Kandungan yang digunakan untuk membuli)*

- (a) There must be a clear definition of cyberbullying in any proposed new laws. It is our position that a definition for cyberbullying should, among others, cover the actions of sending threatening, abusive, or derogatory messages, the dissemination of false or private information, or the creation and sharing of any material through any electronic means, including but not limited to social media, messaging applications, websites, or any other communication platform and/or technology. It is also important that the definition include the element of repetitiveness and persistence, and recognise the possibility that cyberbullying can manifest in multiple forms, and can escalate or move along the spectrum of offline and online spaces. The Online Safety Advocacy Group will make proposals on a definition for cyberbullying in Part 2 of this Memorandum.
- (b) It is also critical that actions to cyberbullying be proportionate to the actual harm (for example, the threat to life, encouragement of self-harm; doxxing) and not undermine the protection of privacy and freedom to expression.

4.1.5 *Kandungan 5 (Kandungan yang boleh mengapiakan violence atau terrorism)*

- (a) Content and measures introduced in the online safety laws should be limited to aggravated forms of violent extremism and terrorism that are likely to (i) cause serious bodily harm to a person; (ii) endanger a person's life; or (iii) cause serious risk to the health and safety of the public.

4.1.6 Kandungan 6 (Kandungan yang berkemungkinan mendorong kanak-kanak untuk menyebabkan kemudaratan kepada diri sendiri (harm themselves))

- (a) The definition of this type of harmful content needs to be aligned with related legislation, including the Child Act 2001, Sexual Offences Against Children Act 2017, and the Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007.

4.1.7 Kandungan 7 (Kandungan yang membangkitkan kebencian (hate speech))

- (a) Any provisions that attempt to deal with incitement to “hate speech” in the Malaysian context, including content that incites or advocates hatred, hostility, discrimination, and violence, should be in compliance with Article 19(3) and Article 20(2) of the International Covenant on Civil and Political Rights (ICCPR) and be required to meet the threshold of the six-part test of the Rabat Plan of Action.

5. Duties under the OSB

5.1 It is our view that certain specific duties and obligations of internet service providers and platform providers must be clearly codified and defined in any online safety laws or regulations. This would include a duty to act responsibly, a duty to protect children, a duty to make priority harmful content inaccessible, and a duty to protect freedom of expression. The duty of care framework that is adopted within online safety laws, while upholding the duty to protect children and other vulnerable groups, should not lead to over-moderation and undermine freedom of expression.

5.2 The independent regulatory body through meaningful consultation with related stakeholders should be mandated to determine and adopt as necessary specific regulations that would operationalise the duties incorporated in the online safety laws.

6. Online Safety Plan under the OSB

6.1 The scope and elements of the online safety plan and the risk assessment by platform providers must be laid out in detail in the online safety laws, and should incorporate elements recommended in the EU Digital Services Act.

6.2 In this regard, it is recommended that the UN Guiding Principles on Business and Human Rights framework be applied to ensure social media platforms:

- (a) avoid causing or contributing to adverse human rights impacts and seek to prevent or mitigate such impacts directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts (principle 13);
- (b) conduct due diligence that identifies, addresses and accounts for actual and potential human rights impacts of their activities, including through regular risk and impact assessments, meaningful consultation with potentially affected groups and other stakeholders, and appropriate follow-up action that mitigates or prevents these impacts (principles 17–19);

- (c) engage in prevention and mitigation strategies that respect principles of internationally recognized human rights to the greatest extent possible when faced with conflicting local law requirements (principle 23);
- (d) conduct ongoing review of their efforts to respect rights, including through regular consultation with stakeholders, and frequent, accessible and effective communication with affected groups and the public (principles 20–21); and
- (e) provide appropriate remediation, including through operational-level grievance mechanisms that users may access (principles 22, 29 and 31).

- Reference: Special Rapporteur on FoE, Report of 6 April 2018, A/HRC/38/35, para 11.

7. Conclusion

7.1 The Government Proposals do not make clear its intended plan of action to ensure alignment between the proposed new online safety laws and other overlapping legislation, such as the Communications and Multimedia Act 1998 (CMA), Personal Data Protection Act 2010 (PDPA), Sedition Act 1948, and other FOE-related laws. It is also unclear how the different forms of regulation of ISPs and social media platforms by different ministries (such as the proposed Code of Conduct that is being developed by the Ministry of Communication on social media licensing) will be harmonised. It is critical that laws rendered obsolete by the introduction of new online safety laws should be repealed or removed. The creation or perpetuation of multiple offences should be avoided.

7.2 These submissions set out in broad strokes the Online Safety Advocacy Group's response to the policy rationale underlying the Government's Proposals. However, it is our preference to present our concerns and recommendations directly to BHEUU and the Law Minister, so that we answer follow up questions as required. Absent the opportunity to do so, we would be happy to provide clarification in writing if required.

7.3 In any event, Part 2 of the Online Safety Advocacy Group's Memorandum will be submitted shortly. We ask that both Part 1 and Part 2 be read together.

Date: 8 October 2024