ARTICLE 19

MALAYSIA

THE COMMUNICATIONS AND MULTIMEDIA ACT 1998

LEGAL ANALYSIS

FEBRUARY 2017

Executive Summary

In February 2017, ARTICLE 19 analysed the Communications and Multimedia Act of Malaysia (the Act) for its compliance with international human rights standards, in particular the right to freedom of expression.

The Act has an expansive scope, ranging from spectrum allocation and consumer protection to content regulation and investigatory powers. The main subjects of regulation under the Act are applications services and network services. The Act further pertains to content applications services, which appear to include online intermediaries. The governmental actors involved in the administration of the Act are "the Minister charged with responsibility for communications and media" and the Malaysian Communications and Multimedia Commission, which is established under the Act.

In the analysis, ARTICLE 19 concludes that the Act creates a number of overly broad content-related offences. In addition, the licensing scheme for network and applications services lacks adequate safeguards against censorship. Finally, the Act introduces far-reaching investigatory powers which are at odds with the protection of journalistic sources and the right to anonymity.

ARTICLE 19 calls on the Malaysian Government to urgently review the Act, introduce necessary amendments and ensure it fully complies with the international freedom of expression standards.

Key recommendations

- Section 211 should be thoroughly revised to more narrowly and precisely define what qualifies as prohibited content under the Act, in line with the three-part test under international law;

- Distinction should be made between private communications and content that is publicly available; the former should be explicitly excluded from the scope of the Act;

- The liability of online intermediaries under the Act should be clarified. Service providers should not be held criminally liable for content produced by others; instead, they should be granted immunity from liability;

- Sections 212 and 213 should clearly set out what the position of the content forum is vis-a-vis other enforcement mechanisms and define its powers in this regard. It should be made explicit that protection of the right to freedom of expression will be part of any self-regulation regime;

- Section 233(1)(a) should be thoroughly revised to more narrowly and precisely define what constitutes "improper use of network facilities or services" under the Act;

- Section 233(1)(b) should be thoroughly revised to narrowly define the circumstances under which anonymous speech can be penalised under the Act;

- Section 233(2) should more precisely and narrowly define what constitutes "obscene" communication and raise the threshold for liability of intermediaries to one of actual and specific knowledge of illegal use of their facilities;

- Section 234 should be redrafted to afford proper protection to legitimate whistle-blowing activities and those involved in journalistic activity who obtain and disclose information and data in the public interest;

- The licensing scheme should:
  - establish clear criteria for the awarding of licenses, as well as the grounds for their withdrawal, eliminating the discretionary powers of government (-appointed) actors in the process;

  - explicitly exclude online intermediaries from the licensing scheme;

  - create an independent regulatory body with full powers to implement the Act's licensing scheme, as well as the ability to receive and resolve complaints about its implementation. Decisions from this regulatory body should be subject to an appeal to an independent and impartial judicial body;

- Sections 74, 75, 247, 248, 249, 254, and 256 should provide clear exemptions to allow for the protection of journalistic sources;

- Section 253 should be redrafted to include an exemption for journalistic material. The exemption should apply to collecting and storing data for the purpose of publishing information, ideas, or opinions believed to be of general public interest;

- Section 252 should be amended to provide clear and narrowly defined grounds for surveillance. Surveillance should only be ordered on the basis of a judicial warrant;

- Section 263 should be abolished. Instead, as a matter of principle, hosting service providers should only be required to remove access to content following a court order, respective of the due process principles.

Table of contents

MALAYSIA : The Communications and Multimedia Act, 1998 Legal Analysis

Introduction

In this legal analysis, ARTICLE 19 reviews the Communications and Multimedia Act of Malaysia (the Act) for its compliance international human rights standards, in particular those on the right to freedom of expression.

ARTICLE 19 is concerned that the Act has been invoked frequently in the recent years to restrict active social media usage in Malaysia. It has been used by law enforcement agencies and the Attorney General of Malaysia to arrest, investigate and charge individuals expressing progressive or dissenting views. At present, a constitutional challenge is being mounted against the Act at the Federal Court.

The Act is not the only piece of legislation that is invoked to suppress freedom of expression in Malaysia, in particular online; other laws include the Sedition Act 1948, S114A of the Evidence Act 1950 and the Film Censorship Act 2002. Often, charges are brought jointly under several laws simultaneously. The most prominent cases of prosecutions include:

- Case of Khalid Ismath who was arrested under Section 233 of the Act in October 2015 for allegedly posting a comment on Facebook. He was charged with 11 alleged offences under the Act and three more charges under the Sedition Act for the same offences. Khalid was subject to several bail conditions including a requirement to report to the nearest police station every 2 weeks, a ban on travel outside of the country and his passport was confiscated by the court; [1]

- Case of Muhammad Amirul who was found guilty of 14 counts of offence under Section 233 of the Act in April 2016 in Kelantan for allegedly insulting a member of the royal family on Facebook. He was initially sentenced to 1 year imprisonment which was later over turned and changed to being sent to a reform school sentence for 2 years; [2]

- Case of Pa Ya (76-year-old man) who was arrested in June 2016 under the Act for allegedly posting an insulting picture on a Whatsapp group chat; [3]

- Case of Sidek Kamiso, a former journalist, who tweeted a critical comment about Haron Din, a deceased PAS spiritual leader, in September 2016. The tweet was deemed to be insulting to Islam and was arrested under Section 233 of the Act in Shah Alam. After the the charges were initially dropped, he was re-arrested under Section 298 of the Penal Code for 'causing religious disharmony' and remains on police bail; [4]

---

1 See, e.g. The Frontline Defenders, The Case of Khalid Mohd Ismath, available at http://bit.ly/2n1DozM.

2 See, SUARAM, http://www.suaram.net/wordpress/wp-content/uploads/2016/12/Overview-2016-Digital-Edition.pdf

3 See, e.g. The Independent, Malaysian pensioner arrested for 'insulting prime minister Najib Razak on Whatsapp', 7 July 2016, available at http://ind.pn/29wu4QF.

4 See, SUARAM, http://www.suaram.net/wordpress/wp-content/uploads/2016/12/Overview-2016-Digital-Edition.pdf

- In February 2016, the Malaysian Communications and Multimedia Commission (MCMC) used its powers for the first time to blanket block websites that published content related to Malaysia's 1MDB scandal. On 25 February 2016, popular online news portal, The Malaysian Insider (TMI) was blocked by the government.[5] Further, blocking of news sites like Sarawak Report[6] and Asia Sentinel;[7] the on-going intimidation and lawsuits against media such as Malaysiakini; and the arrest and deportation of two Australian Broadcasting Corporation journalists are part of a worsening crackdown on media freedom. This was also seen during the recent Sarawak state election with the barring of a foreign journalist from UK Channel 4 News, from a post-election press conference attended by the prime minister.

ARTICLE 19 reviewed the Act as it serves as a 'catch-all' legislation and the legislation that enables the interception of the communication, tracking and ultimately prosecution. The Act has an expansive scope, ranging from spectrum allocation and consumer protection to content regulation and investigatory powers. The main subjects of regulation under the Act are applications services and network services. The Act further pertains to content applications services, which appear to include online intermediaries. The governmental actors involved in the administration of the Act are "the Minister charged with responsibility for communications and media" and the Malaysian Communications and Multimedia Commission, which is established under the Act.

ARTICLE 19 calls on the Malaysian Government to introduce the necessary amendments to the Act and ensure it fully complies with the international freedom of expression standards. We stand ready to provide further assistance in this process.

---

5 See, e.g. the BBC, Blocked Malaysian Insider news website shuts down, 14 March 2016, available at http://bbc.in/1pkjRKR.

6 See, e.g. TechInAsia, Despite being blocked in Malaysia, Medium stands by Sarawak Report, 27 January 2016, available at http://bit.ly/2lT4UOe.

7 See, e.g. Digital Right Monitor, Asia Sentinel blocked by Putrajaya following reports critical of Prime Minister Najib Abdul Razak, available at http://bit.ly/2mxgmTE.

Applicable international standards

The right to freedom of expression

Freedom of expression is one of the bedrock principles of democracy and human rights. It has consistently been described as "one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfillment."[8] The UN Human Rights Committee further stated that freedom of expression is "a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights," for whose enjoyment it forms an essential basis.[9]

The right to freedom of expression is guaranteed by Article 19 of the Universal Declaration of Human Rights[10] (UDHR) and is strongly protected – also under Article 19 – of the International Covenant on Civil and Political Rights[11] (ICCPR), as well as in regional human rights instruments.[12]

The UDHR is not a binding treaty but a recommendatory resolution adopted by the UN General Assembly. Through time and universal acceptance, however, much of the UDHR has risen to the level of customary international law, including Article 19, and is therefore binding on all states.

ARTICLE 19 is aware that Malaysia has neither signed nor ratified the ICCPR. As such, the standard developed under Article 19 of the ICCPR as well as comparative jurisprudence and authoritative statements from international and bodies presented in this analysis are not formally binding on Malaysia. However, it is suggested that the guarantee of the right to free speech in Article 10 para 1 of the Constitution of Malaysia allows wide scope for interpretation. Given the fundamental importance of the right to freedom of expression, and its recognition in the Malaysian Constitution, it is of the utmost importance that every effort be made to ensure that Malaysian laws are interpreted, to the extent possible, in a manner that respects freedom of expression. Jurisprudence from international and regional human rights bodies, as well as non-binding standard-setting documents, such as authoritative international declarations and statements, illustrate the manner in which leading judges and other experts have interpreted international and constitutional guarantees of freedom of expression. As such, they are authoritative evidence of generally accepted understandings of the scope and nature of all international guarantees of freedom of expression. They also provide strong guidance regarding interpretation of the guarantees of freedom of expression found in the Constitution of Malaysia.

---

8 European Court of Human Rights, Lingens v. Austria, Application no. 9815/82, 8 July 1986.

9 UN Human Rights Committee, General comment No. 34, Article 19: Freedoms of opinion and expression (General Comment 34), 12 September 2011, CCPR/C/GC/34, para 2-3.

10 Universal Declaration of Human Rights, 10 December 1948, GA res. 217A (III), UN Doc A/810 at 71 (1948).

11 International Covenant on Civil and Political Rights, 16 December 1966, UN Doc. A/6316 (1966).

12 These include the European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5; the American Convention on Human Rights, 12 November 1969, OAS Treaty Series No. 36, the African (Banjul) Charter on Human and Peoples' Rights, 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5; and the ASEAN Human Rights Declaration, 18 November 2012.

Restriction on the right to freedom of expression

Under international freedom of expression standards, the right to freedom of expression may only be restricted if specific conditions are met:[13]

- The restriction must be **provided by law**. For a norm to be characterised as "law" it needs to be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public.[14] It needs to provide sufficient guidance to those charged with its execution to enable them to determine what type of expression is restricted and what not. Importantly, the UN Human Rights Committee states: "A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."[15]

- The restriction may only be imposed for one of the following legitimate grounds: respect for the rights or reputations of others, and the protection of national security, public order (ordre public), public health or moral. Freedom of expression can be permissibly restricted only for one of these **legitimate aims** and restrictions on other grounds are never in accordance with international law.

- The restriction must conform to the strict tests of **necessity and proportionality**. To meet the requirement of necessity and proportionality, the restriction must be necessary for a legitimate purpose and not be overbroad. The UN Human Rights Committee specified this as follows:

> ***Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected ... The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law.***[16]

The right to privacy

The right to privacy is also well-established under international law. It is internationally recognised by Article 12 of the UDHR and Article 17 of the ICCPR. It is further protected under the following regional human rights instruments.[17]

---

[13] General Comment 34, op.cit., para 22.

[14] Ibid., para 24.

[15] Ibid.

[16] UN Human Rights Committee, General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9, para 14. See also General Comment 34, op.cit., para 34.

[17] See, the European Convention on Human Rights (Article 8), American Convention on Human Rights (Article 11), and the ASEAN Declaration (Article 21).

Restriction on the right to privacy

The wording of Article 17 ICCPR prohibits "arbitrary and unlawful" interferences with the right to privacy. Under international human rights law, restrictions to the right to privacy can only be permissible if the same test is met as that applicable to Article 19. The UN Special Rapporteur on promotion and protection of human rights while countering terrorism stated this as follows:

> ***Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17. Consequently, limitations to the right to privacy or other dimensions of article 17 are subject to a permissible limitations test, as set forth by the Human Rights Committee in its general comment No. 27.***[18]

This has also been clearly set out by the UN Human Rights Committee[19] and UN Commission on Human Rights.[20]

Independence of regulatory bodies

The guarantee of freedom of expression applies with particular force to the media, including broadcast media and the relevant regulatory bodies. The need for protection of regulatory bodies against political or commercial interference was specially emphasised in the 2003 Joint Declaration of the UN Special Rapporteur on Freedom of Expression, the OAS Special Rapporteur on Freedom of Expression and the OSCE Special Representative on Freedom of the Media, who considered:

> ***All public authorities which exercise formal regulatory powers over the media should be protected against interference, particularly of a political or economic nature, including by an appointments process for members which is transparent, allows for public input and is not controlled by any particular political party.***[21]

Guaranteeing the independence of a regulator in practice involves various aspects. ARTICLE 19's publication Access to the *Airwaves: Principles on Freedom of Expression and Broadcast Regulation*,[22] a set of guidelines based on comparative constitutional law and best practice in countries around the world, considers the following to be important:

---

[18] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 28 December 1999, A/HRC/13/37.

[19] UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

[20] UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4.

[21] International Mechanisms for Promoting Freedom of Expression, Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 18 December 2003.

[22] ARTICLE 19, Access to the Airwaves: Principles on Freedom of Expression and Broadcast Regulation, March 2002.

[The] institutional autonomy and independence of broadcast and/or telecommunications [regulatory bodies] should be guaranteed and protected by law, including in the following ways:

1. specifically and explicitly in the legislation which establishes the body and, if possible, also in the constitution;
2. by a clear legislative statement of overall broadcast policy, as well as of the powers and responsibilities of the regulatory body;
3. through the rules relating to membership;
4. by formal accountability to the public through a multi-party body; and
5. in funding arrangements.

Media pluralism

Under international law, States are required to promote media pluralism. In this connection, the establishment of an independent regulator is a key to ensuring plurality and diversity. This was confirmed in the Joint Declaration on Promoting Diversity in the Broadcast Media adopted in 2007 by the special mandates for the protection of freedom of expression of the UN, OSCE, OAS and African Commission, which stated:

> ***Regulation of the media to promote diversity, including governance of public media, is legitimate only if it is undertaken by a body which is protected against political and other forms of unwarranted interference, in accordance with international human rights standards.*** [23]

Other aspects of the promotion of pluralism include equitable access to the airwaves, fair and transparent licensing processes, and the prevention of undue media ownership concentration.

[23] International Mechanisms for Promoting Freedom of Expression, Joint declaration on the diversity of broadcasting by Rapporteurs of the UN, the OSCE, the OAS and the ACHPR, 14 December 2007.

Analysis of the Act

ARTICLE 19 observes that the Act has an expansive scope. In this analysis, we focus on the most problematic provisions from the human rights perspective and urge the Government to urgently amend them.

Content-related offences

Indecent, obscene, false, menacing, or offensive content

The most problematic content-related offence is laid down **Section 211** of the Act, which prohibits "offensive content" as follows:

> ***No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person."***

ARTICLE 19 makes the following comments on these provisions:

- **The provisions do not meet the test of legality:** None of the elements of this prohibition – "indecent", "obscene", "false", "menacing", or "offensive in character with intent to annoy, abuse, threaten or harass any person" – are defined further in the Act. This creates a potentially endless category of offences, which are at the discretion of law enforcement to define further.

As set out above, in order for legislation to meet the legality criterion, the law must be formulated with sufficient precision to enable an individual to regulate his or her conduct. The law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. ARTICLE 19 observes that the vague and overly broad manner in which Section 211 is currently drafted fails to meet that standard. The key elements of the provision are, in their current form, near-infinite in scope and hinge upon highly subjective terms that are open to a broad range of interpretation.

- **The restrictions do not pursue legitimate grounds:** As noted above, restrictions on freedom of expression must serve a legitimate legislative objective which is of sufficient importance to justify limiting a fundamental right. Typically, the prohibition of certain materials could be legitimate on the grounds of public morals, e.g. if the aim is the prevention of harm to children. It is much less clear that the objective of preventing offence to public sensibilities warrants restricting freedom of expression.

Courts in many jurisdictions have distinguished 'offensive' material from material that is actually harmful, only allowing restrictions which have as their objective the prevention of harm.

For example, from the comparative perspective, the European Court of Human Rights, for example, has stated that freedom of expression is applicable "to 'information' or 'ideas' that ... offend, shock or disturb the State or any other sector of the population."[24] Historically, States have often been guilty of a form of paternalism in applying restrictions on sexually explicit material. Such paternalism is inconsistent with human rights guarantees, including freedom of expression, which presume that all adults are equal and responsible moral agents. It is not for a judge, or even elected officials, to decide what materials we should or should not be able to access, in the absence of a real risk of actual harm.

ARTICLE 19 is firmly of the opinion that any obscenity restrictions must be aimed at preventing real harm and not simply at preventing 'offence to public sensibilities', sometimes misleadingly described as 'harm to public morals'. In general, this means that expressions - pictures, films and so on - of activities that are themselves legal, should also be legal. Obviously this applies only where the production of the expression is itself legal and any individuals involved are acting by consent.

- **The restrictions are disproportionate:** The lack of clarity is exacerbated by the criminal penalties that can be imposed: a fine, imprisonment up to one year, and additional fines for "every day or part of a day during which the offence is continued after conviction." This also raises concerns about the necessity and proportionality criterion: under the current Section 211, content that is considered "annoying" by one person – no matter how acceptable the expression might be by objective standards and no matter if it concerns a matter of public interest – can lead to the lengthy, disproportionate imprisonment of another.

- **Intermediary liability:** "Content applications" are defined in Section 6 as "a service provided by means of, but not solely by means of, one or more network services" and "content applications service" as "an applications service which provides content". An "applications service provider" is in turn defined as "a person who provides an applications service", and "content" as "any sound, text, still picture, moving picture or other audio-visual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved or communicated electronically." Content applications service providers therefore appear to include online intermediaries.

The prohibition in Section 211 seems to apply to private communications in addition to publicly available content as no explicit distinction is made between the two. It also appears to offer the possibility of holding online intermediary services strictly liable for user-generated content. This is against international freedom of expression standards.

ARTICLE 19 notes that intermediaries, such as Internet Service Providers (ISPs), search engines, social media platforms and web hosts, play a crucial role in relation to access to the Internet and transmission of third party content. They have come to be seen as the gateways to the Internet without which most people would not be able to gain access to information online.

[24] Handyside v. United Kingdom, 7 December 1976, 1 EHRR 737, para 49.

Because of this crucial position, many countries have granted Internet intermediaries complete or conditional immunity for third-party content.[25] They have also been exempted from monitoring content.[26] Accordingly, the four special rapporteurs on freedom of expression recommended in their 2011 Joint Declaration on Freedom of Expression and the Internet that:

- No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;
- Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;
- ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[27]

Recommendations

- Section 211 should be thoroughly revised to more narrowly and precisely define what qualifies as prohibited content under the Act, in line with the three-part test under international law;
- Distinction should be made between private communications and content that is publicly available; the former should be explicitly excluded from the scope of the Act;
- The liability of online intermediaries under the Act should be clarified. Service providers should not be held criminally liable for content produced by others; instead, they should be granted immunity from liability.

"Content forum"

The subsequent **Sections 212 and 213** create the possibility for self-regulation via a so-called "content forum" that should regulate the takedown of offensive content. However, these provisions do not appear to create any specific powers for the content forum that could not already be achieved through civil law. The policies of such a forum could potentially raise free speech concerns as currently no mention is made of the right to freedom of expression.

---

[25] See for example, for a comparative perspective, the Electronic Transaction Act 2010 of Singapore which gives strong protection to innocent providers; or the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, the E-Commerce Directive in the EU.

[26] See, for comparative perspective, Article 15 of the E-commerce directive. In the case of SABAM v. Scarlet Extended SA, the Court of Justice of the European Union considered that an injunction requiring an ISP to install a filtering system to make it absolutely impossible for its customers to send or receive files containing musical works using peer-to-peer software without the permission of the rights holders would oblige it to actively monitor all the data relating to each of its customers, which would be in breach of the right to privacy and the right to freedom to receive or impart information. The court noted that such an injunction could potentially undermine freedom of information since the suggested filtering system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.

[27] See, Joint Declaration on Freedom of Expression and the Internet, Declaration signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011; available at http://www.osce.org/fom/78309.

It is also unclear if the content forum procedures would take precedence over the criminal law proceedings provided for elsewhere in the Act.

Recommendations

- Sections 212 and 213 should clearly set out what the position of the content forum is vis-a-vis other enforcement mechanisms and define its powers in this regard. It should be made explicit that protection of the right to freedom of expression will be part of any self-regulation regime.

Improper use of network facilities or service

Section 233 on the "improper use of network facilities or network service" contains similar language as Section 211. The concerns outlined above regarding the wording of that provision equally apply to Section 233(1)(a), which also fails to meet the legality standard and, due to the imposition of criminal measures including imprisonment, raises concerns regarding necessity and proportionality.

Section 233(1)(b) specifically focuses on anonymous expression by proscribing "[initiating] a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address." This provision appears to penalise anonymous speech.

ARTICLE 19 notes that under international law, the protection of anonymity online has been linked to the protection of privacy and personal data. In the words of the UN Special Rapporteur on freedom of expression: "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief."[28] In similar vein, the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights found that "the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions."[29]

Restrictions to anonymity must meet the three-part test, outlined above.[30] As discussed for Section 211, the wording used there, which is repeated in Section 233(1)(b), fails to meet the standard of legality and also raises concerns regarding necessity and proportionality. Section 233(1)(b) falls even further short on the legality test as it also covers what can be described as "attempted communication": it proscribes expression "during which communication may or may not ensue" (emphasis added). With its vague and overly broad wording, Section 233(1)(b) could be considered as a blanket ban of anonymous speech. The UN Special Rapporteur has stated that "blanket prohibitions [of anonymity] fail to be necessary and proportionate."[31]

Section 233(2) prohibits knowingly using a network service or applications service to provide "obscene" communication to a person for commercial purposes or permitting a "network service or applications service under the person's control" to be used for that purpose. Ostensibly, this is an anti-pornography provision. As set out in the discussion on Section 211, the term "obscene" is not further defined in the Act, leaving the provision open to a broad range of interpretation and thereby violating the principle of legality.

---

[28] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, 29 May 2015 (2015 UN SR Report), para 12. See also para 16.

[29] Organization of American States, press release 17/15.

[30] 2015 UN SR Report, op.cit., para 31.

[31] Ibid., para 60.

In contrast to Section 211, a knowledge standard is set for intermediary services as anyone permitting a network service or application service to be used for obscene communication needs to do so "knowingly". Nevertheless, this still creates substantial risk for these services as the standard of knowledge is framed in very general terms. This arguably means that only general knowledge of illegal activity is required to incur criminal liability under the Act, rather than specific and actual knowledge.

Recommendations

- Section 233(1)(a) should be thoroughly revised to more narrowly and precisely define what constitutes "improper use of network facilities or services" under the Act;
- Section 233(1)(b) should be thoroughly revised to narrowly define the circumstances under which anonymous speech can be penalised under the Act;
- Section 233(2) should more precisely and narrowly define what constitutes "obscene" communication and raise the threshold for liability of intermediaries to one of actual and specific knowledge of illegal use of their facilities.

Interception of communication

Section 234 prohibits the interception of any communication and the disclosure and use of such communications. Interception is broadly defined in Section 6, as "the aural or other acquisition of the contents of any communications through the use of any electronic, mechanical, or other equipment, device or apparatus."

Furthermore, disclosure is prohibited for all information which someone would "have reason to believe" was obtained through unlawful interception.

ARTICLE 19 finds that this casts an impermissibly wide net that, amongst others, could be used to counter legitimate whistle-blowing activities. The Act should exempt disclosures that are justified as being in the public interest, as well as disclosures made with the reasonable belief that they are made pursuant to a right or duty.

Recommendation

- Section 234 should be redrafted to afford proper protection to legitimate whistle-blowing activities and those involved in journalistic activity who obtain and disclose information and data in the public interest.

Licensing

The Act creates an elaborate licensing scheme for network services and application services **(Section 126)**, and an additional licensing scheme for content application services **(Section 205)**. It operates through categorical "class licenses", which cover general types of services, as well as "individual licenses" that can be granted on an ad hoc basis. Those under a class license still have a duty to register with the Commission **(Sections 45 and 131)**. Providing a service without a license is an offence punishable by a prison sentence of up to five years.

A significant problem with the network services and application services license system relates to a lack of foreseeability and predictability, and a lack of independent oversight. The Act does not set up clear criteria for eligibility, and permits the Minister to impose additional requirements

for or conditions on licenses **(Sections 13, 16(b), 30, 127)**. The Minister may also draw up lists of persons or classes of persons who are ineligible to apply **(Section 27(2))**. No further grounds on the basis of which the Minister can bar certain classes from applying are provided in the Act. The Minister may also cancel existing licenses under a highly permissive "public interest" test (Section 38 and 37(e)) or if the licensee has failed to comply with "any instrument issued, made or given by the Minister or the Commission" **(Section 38 and 37(d))**. The Commission may do the same for persons registered to a class license **(Section 47(d) and (e))**.

The Act does not provide for any checks and balances to these elaborate powers. The only requirement the Minister appears to need to adhere to is that of giving prior notice and stating reasons for any action taken **(Section 13)**. The licensing system therefore amounts to a broad and largely unconditional power of censorship of practically all media operations in the country.

An additional problem is that network services are also subject to regime, extending the licensing regime to the online sphere. This is generally considered as contrary to international law. As the joint special mechanisms on freedom of expression stated:

> ***Licensing, justified by reference to the airwaves as a limited public resource, is not legitimate for Internet broadcasting.***[32]

While the content application licensing scheme does create certain categorical exemptions for "incidental", "closed" and "limited" services **(Sections 207-209)**, the definitions of these concepts are rather imprecise **(Section 6)** and do not seem to assuage the more fundamental concern with the licensing regime as a whole.

All licenses are subject to standard license conditions, listed in **Schedule 1** of the Act. These include additional requirements, including a duty of incorporation within Malaysia, foreign investment restrictions, and various notification duties (although the Minister can create exemptions pursuant to **Section 213**).

An overarching shortcoming is the **complete lack of independence** of those tasked with overseeing the licensing system: the Minister and the Commission. The Commission performs a wide range of administrative and quasi-judicial tasks under the Act, ranging from the processing of class license registrations, to dispute resolution, to spectrum and number allocation. Curiously, the Act does not provide any explicit details on the establishment of the Commission and/or the appointment of its members. This raises questions regarding the Commission's independence.

The Act also foresees in the possibility for the Minister to establish an Appeal Tribunal **(Section 17)**. However, this body appears to lack any significant independence as well. Tribunal members are appointed by the Minister directly and can be dismissed by the Minister on wide-ranging and subjective grounds, including on the basis that a tribunal member's performance has been "unsatisfactory" for a significant period of time **(Section 20(1)(h))**.

As set out above, international law requires that bodies exercising regulatory powers over the media are independent from government.

[32] See The 2011 Joint Declaration, op.cit.

Under the Act, however, the main actor implementing the licensing system is the Minister, with the assistance of a Commission that is acting under the Minister's direction (see, for example, **Section 10(3))**. The lack of an independent regulatory body, combined with the near-complete absence of any checks and balances to the Minister's power, raises serious concerns about the likelihood that the Act's licensing scheme will be implemented consistently and effectively across the board.

Recommendations

- The licensing scheme should:
  - establish clear criteria for the awarding of licenses, as well as the grounds for their withdrawal, eliminating the discretionary powers of government (-appointed) actors in the process;
  - explicitly exclude online intermediaries from the licensing scheme;
  - create an independent regulatory body with full powers to implement the Act's licensing scheme, as well as the ability to receive and resolve complaints about its implementation. Decisions from this regulatory body should be subject to an appeal to an independent and impartial judicial body.

Protection of sources

The Act creates various powers for the Commission and law enforcement to gather information and request documents, often coupled with penalties for those who refuse to comply. A recurring problem with these provisions is the lack of safeguards or exemptions for the protection of journalistic sources.

- **Section 256** allows for oral examinations to be conducted without a requirement of reasonable suspicion. Refusing to give information relating to an offence constitutes an offence, punishable with a fine, a maximum of six months' imprisonment, or both **(Section 241)**. A person may refuse to answer questions to avoid self-incrimination, but not for any other purpose, such as the protection of a source **(Section 256(2))**.

- Under **Sections 74 and 75**, the Commission may request information or any document from any person if it has "reason to believe" it is relevant to the performance of its duties. Non-compliance and failure to disclose constitute an offence. This is a very low threshold to request information and documentation, especially since no exemptions – such as the protection of journalistic sources ¬– are provided for.

- Law enforcement officers are also empowered to conduct searches and seize documents from any premise under **Section 247**. This requires a warrant unless they have reasonable cause to believe that delay would "adversely affect the investigation" **(Section 248)**. This authority extends to computer systems, and thus to require "being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data" **(Section 249)**. Similarly, **Section 254** lays down an additional power to "require the production of records", refusal of which is once more punishable as an offence.

- Another problematic provision is **Section 253**, which broadly prohibits impeding, obstructing or interfering with any investigation. This could have ramifications for preventative measures such as encryption, which can be essential to protect confidentiality of sources. The UN Special Rapporteur has stated the following:

> ***States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.***[33]

Limits on privacy affect the ability of the media to operate. Journalists are not able to effectively pursue investigations and receive information from confidential and other sources.[34] Section 253 in its current form constitutes an obstacle to journalists in gathering, storing and protecting their journalistic material.

---

[33] 2015 UN SR Report, op.cit., para 59.

[34] See e.g. IFEX Alert, Thirty IFEX members call on governments to respect fundamental human rights of free expression and privacy of communications, 5 June 2009. http://www.ifex.org/international/2009/06/05/ja_gm/.

[35] Necessary and Proportionate Coalition, Necessary & Proportionate, May 2014, available at http://necessaryandproportionate.org/principles.

Recommendations:

- Sections 74, 75, 247, 248, 249, 254, and 256 should provide clear exemptions to allow for the protection of journalistic sources;
- Section 253 should be redrafted to include an exemption for journalistic material. The exemption should apply to collecting and storing data for the purpose of publishing information, ideas, or opinions believed to be of general public interest.

Surveillance

Section 252 creates a power to intercept "any communications", where the Public Prosecutor considers it "likely" to contain any information which is relevant for the purpose of any investigation into an offence under the Act, or its subsidiary legislation. The powers given to the Public Prosecutor are very broad:

> ***Notwithstanding the provisions of any other written law, the Public Prosecutor, if he considers that any communications is likely to contain any information which is relevant for the purpose of any investigation into an offence under this Act or its subsidiary legislation, may, on the application of an authorised officer or a police officer of or above the rank of Superintendent, authorise the officer to intercept or to listen to any communication transmitted or received by any communications.***

This provision raises concerns regarding necessity and proportionality in relation to the right to privacy, as well as regarding the right to freedom of expression.

ARTICLE 19 suggests that the Malaysian legislators should take a note of the Necessary & Proportionate Principles that set out in a detailed manner what the requirement of proportionality entails in the surveillance context, given the grave interference with the right to privacy that it constitutes:

Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

- there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;
- there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and;
- other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option, and;
- information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
- any excess information collected will not be retained, but instead will be promptly destroyed or returned, and;
- information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given; and
- that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.[35]

The low threshold required for the Public Prosecutor to order surveillance measures – if they think communications are "likely" to contain certain information – combined with the overly broad and vaguely defined offences under the Act ¬ such as the "offensive" content proscribed by Section 211 – allow for the invasive measure of surveillance to be taken for relatively minor infractions under the Act. This raises significant concerns of necessity and proportionality. This is in addition to the clear violation of the legality criterion that Section 252 poses, with wording that includes vague terms such as "any information" and "any offence", which leave unfettered discretion to the Public Prosecutor for their interpretation.

International law requires that the use of surveillance powers by public officials must not only be necessary and proportionate, but also independently overseen to safeguard against abuse. The Necessary & Proportionate Principles state that "determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent."[36] This is related to the principle of due process, meaning that surveillance decisions must not only be made in accordance with the law, but also in a manner that is compatible with the fundamental rights of the data subject.[37] The Public Prosecutor's discretionary powers to order surveillance measures without obtaining a warrant fall short of this requirement.

In addition to the shortcomings of the surveillance powers in light of the international law obligations regarding the right to privacy, the existence of surveillance practices in and of itself also has a chilling effect on the right to freedom of expression.[38] In the words of the UN Special Rapporteur on freedom of opinion and expression:

> Even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse.[39]... States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy.[40]

Recommendation

- Section 252 should be amended to provide clear and narrowly defined grounds for surveillance. Surveillance should only be ordered on the basis of a judicial warrant.

General duty of licensees

The Section 263 establishes a duty of licensees to "use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia." Further, upon written request of the MCMA or any other authority, the licensees must assist the authorities "as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security."

---

[36] Ibid.

[37] Ibid..

[38] UDHR.

[39] The 2015 UN SR Report, op.cit., para 52.

[40] Ibid., para 79.

The provisions of Section 263 are extremely problematic as they require intermediaries to monitor content in order to comply with the Malaysian law. This essentially amounts to imposing on them a duty of care in respect of preventing the transmission of unlawful material. As such, they are given a strong incentive to actively monitor and filter information on their services in order to locateinfringing material. In this way, the provisions of Section 263 are deeply inimical to freedom of expression and the free flow of information on the Internet.

ARTICLE 19 has long condemned the provisions requiring the intermediaries to monitor the content on the ground that in the vast majority of cases, they lack a clear legal basis and fail to provide for minimum due process safeguards. The provisions of Section 263 are no exception:

- Lack of clarity: Section 263 provides no clarity how the provisions should be applied, something which is likely to lead to inconsistent practices and ultimately legal uncertainty for Internet intermediaries. The term "prevention" is also unclear. We are aware that in practice, as long as Malaysian authorities believe that a website is a potential threat, it orders to block a particular website, despite the fact that no offence has been proven to have been committed;

- Lack of due process safeguards: The Act provides no minimum due process safeguards that are necessary to protect the right to freedom of expression of Internet users

- In addition, ARTICLE 19 believes that the requirement under Section 263 will have a chilling effect on freedom of expression since intermediaries tend to err on the side of caution by over-censoring potentially unlawful content.

ARTICLE 19 notes that international bodies have also commented on liability regimes for intermediaries. For example, in their 2011 Joint Declaration on Freedom of Expression and the Internet, the four special rapporteurs on freedom of expression recommended that:

No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;

Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;

ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[41]

[41] The 2011 Joint Declaration, op.cit.

Similarly, in 2011, the UN Special Rapporteur on freedom of expression stated that:

> Censorship measures should never be delegated to a private entity, and […] no one should be held liable for content on the internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf.[42]

He further recommended that, in order to avoid infringing internet users' right to freedom of expression and right to privacy, intermediaries should only implement restrictions to these rights after judicial intervention; that intermediaries should be transparent about measures taken with the user involved and, where applicable, with the wider public; that they should provide, if possible, forewarning to users before implementing restrictive measures; and they should strictly minimise the impact of any restrictions to the specific content involved.[43] Finally, the Special Rapporteur has emphasised the need for effective remedies for affected users, including the possibility of appeal using procedures to be provided by the intermediary and by a competent judicial authority.[44]

In ARTICLE 19's view, Section 263 should be abolished. Instead, the Malaysian law should grant broader immunity to hosting providers. They should be almost fully insulated from liability for third-party content except where required to comply with a court order and as long as they do not interfere with that content so that they should only be required to remove unlawful material following a court order.

Recommendation :

- Section 263 should be abolished. Instead, as a matter of principle, hosting service providers should only be required to remove access to content following a court order, respective of the due process principles.

[42] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27, para. 43.
[43] Ibid., para 47.
[44] Ibid.

ABOUT ARTICLE 19

ARTICLE 19 was founded in 1987. We are registered and regulated in the UK (charity number 327421), Bangladesh, Brazil, Kenya, Mexico, Senegal, Tunisia and the USA.

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvementsin proposed or existing domestic legislation. All of our analyses are available at **http://www.article19.org/resources.php/legal**.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at **legal@article19.org**. For more information about the ARTICLE 19's work in Malaysia, please contact Nalini Elumalai,