Module 7

CYBERCRIMES

Modules on Litigating Freedom of Expression and Digital Rights in South and Southeast Asia

MEDIA DEFENCE

Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of the Centre for Law and Democracy (https://www.law-democracy.org/live/) and ALT Advisory (https://altadvisory.africa/)

June 2022

In partnership with

TABLE OF CONTENTS

MODULE 7

CYBERCRIMES

- **As access to the internet continues to grow rapidly in Asia, cybercrimes are becoming ever more prevalent and dangerous.**
- **However, laws which regulate criminal activity on the internet, or cybercrimes laws, are increasingly providing tools for the state to suppress dissent and the media.**
- **Data privacy is starting to attract more widespread attention across Asia, with many countries recently passing data protection laws, albeit often containing insufficiently robust privacy protections.**
- **Concerningly, many cybercrimes have a particularly gendered nature, such as cyberstalking and the non-consensual dissemination of intimate images.**
- **There are various practical steps that can be taken to address online harms and ensure that fundamental rights are equally protected both off- and online.**

INTRODUCTION

The increase in internet access recently has created a number of new legal challenges. The internet is transnational and ubiquitous, and the new landscape created by the digital world has raised novel challenges when it comes to protecting fundamental rights in the digital age. Old definitions about what constitutes a publisher or a journalist are increasingly complicated; the anonymity afforded by many internet platforms, while key to fostering freedom of expression in many contexts, can pose challenges in relation to combatting illegal online activities and seeking remedies for victims; and there are serious questions about who is liable for content shared online that may affect parties in different jurisdictions in some way.

Regulating and legislating crimes that occur on, or relate to, the internet has been a difficult undertaking for states and international bodies. In 2020, global cybercrimes costs were forecast by the research group Cybersecurity Ventures to grow by 15 per cent annually, predicted to reach USD 10.5 trillion annually by 2025.[1] Without adequate regulatory frameworks and protections, the growth of internet access, e-commerce and economic development may continue to fuel the spread of cybercrime.

In Asia, where the number of new internet users continues to grow at a rapid rate, the increase in access to the internet and information and communications technologies (ICTs) has also led to increased criminal activity online. However, laws to regulate criminal activity on the internet are

[1] Global News Wire, 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025' (2020) (accessible at: https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html).

increasingly providing tools for the state to suppress dissent or to punish critics and independent media because of their often vague and overly broad nature.

As far back as 2011, the United Nations (UN) Special Rapporteur on freedom of expression warned:

> "[L]egitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the internet. Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice are used to censor content that the Government and other powerful entities do not like or agree with."[2]

Unfortunately, the problem has only gotten worse since then.

WHAT IS A CYBERCRIME?

Definition

There is no precise, universal definition of the term 'cybercrime'. In general terms, it refers to a crime that is committed using a computer network or the internet.[3] This can cover a wide range of activities, including terrorist activities and espionage conducted with the help of the internet, illegal hacking into computer systems, content-related offences, theft and manipulation of data, and cyberstalking.[4]

Cybercrimes and cybersecurity are two issues that cannot be separated in an interconnected digital environment. Cybersecurity, or the protection of digital devices, systems and networks against cybercrimes, refers to the collection of "tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets", such as computing devices, applications and telecommunication systems.[5]

Cybercrimes in international law

The UN General Assembly Resolution on the Creation of a global culture of cyber security states:

> "Security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency."[6]

---

[2] United Nations General Assembly, Human Rights Council, 17th Session, 'Report of the Special Rapporteur on freedom of expression' at p. 10 (2011) (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
[3] Article 19, 'Freedom of Expression and ICTs: overview of international standards' at p. 25 (2018) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf).
[4] *Id.*
[5] ITU Definition of Cybersecurity, (accessible at: https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx).
[6] UN General Assembly, Fifty-seventh session, 'Resolution on the Creation of a global culture of cyber security, at p 3 (accessible at: https://digitallibrary.un.org/record/482184?ln=en).

The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on cybercrime.[7] This Convention is open for adoption by states outside of Europe, and to date, the Philippines and Sri Lanka are the only two states in South and Southeast Asia that are party to it.[8] The Budapest Convention has also been used as a 'model law' for legislators in certain jurisdictions. For example, Sri Lanka modelled its 2007 national legislation, the Computer Crime Act, on the Budapest Convention prior to being invited in 2015 to join the Convention.[9]

Although it has been cited as a 'benchmark' by certain participants in current negotiations for a UN convention on cybercrime, the Budapest Convention has been criticised for providing insufficient procedural protections for the rights to freedom of expression and privacy, and for containing superfluous and overbroad content and copyright offences.[10]

Cybercrimes in domestic law

Cybercrimes legislation has proliferated across South and Southeast Asia in recent years despite only two states in the region being party to the Budapest Convention.

To ensure that cybercrimes laws do not unnecessarily infringe on the fundamental rights to freedom of expression, privacy and access to information, legislation should meet the following criteria:

- Provide narrow and clear definitions of cybercrimes, well-tailored to advancing legitimate aims and minimally restrictive of freedom of expression and privacy rights.
- Require proof about the likelihood of harm arising from a given criminal activity.
- Require the nature of the threat resulting from any criminal activity to be identified.
- Not introduce different standards for online and offline behaviour unless that behaviour is fundamentally different online.
- Provide for a public interest defence in relation to the obtaining and dissemination of information classified as secret.
- As a general principle, not impose prison sentences for expression-related offences, except for those permitted by international legal standards and with adequate safeguards against abuse.[11]

---

[7] Council of Europe, 'Budapest Convention and Related Standards', (accessible at: https://www.coe.int/en/web/cybercrime/the-budapest-convention).
[8] Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY' (https://www.coe.int/en/web/cybercrime/parties-observers?wpisrc=nl_cybersecurity202).
[9] Council of Europe, Cybercrime Convention Committee (T-CY), 'The Budapest Convention on Cybercrime: benefits and impact in practice' (2020) at section 4.2.2, p. 30 (accessible at: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac).
[10] See Article 19's briefing, 'The Council of Europe Convention on Cybercrime and the First and Second Additional Protocol' (2022) (accessible at: https://www.article19.org/wp-content/uploads/2022/06/Budapest-Convention-analysis-May-2022.pdf).
[11] Media Defence, 'Training manual on digital rights and freedom of expression online, at pp 62 (2020) (accessible at: https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-digital-rights-and-freedom-of-expression-online/).

TYPES OF CYBERCRIMES

Data privacy violations

The use of data, including the volume of cross-border data flows, is increasing every year, and this includes personal data. However, there is a lack of adequate regulations in many countries for the collection and processing of personal information which can have significant ramifications, making data protection laws critical. In recent years, increasing attention to the issue of data protection has led to a number of Asian states enacting new privacy laws.[12] However, many states continue to protect individuals' privacy only inadequately, especially from state surveillance activities.[13]

The rise of sophisticated surveillance technologies and the use of biometric technologies without proper safeguards are just some of the many threats to the right to privacy across Asia. There have, however, been some encouraging judgments in recent years pointing to the willingness of the judiciary in certain states to protect the right to privacy.

The Supreme Court of India on 'Pegasus' spyware

In *Manohar Lal Sharma v. Union of India*[14] the Supreme Court of India considered the alleged involvement of the Indian government in the unauthorised use of Pegasus spyware software to engage in mass surveillance. The petitioners in *Manohar* (a mix of public interest litigants and those claiming to be victims) alleged that the government's unauthorised use of Pegasus was a violation not only of rights to privacy but also of freedom of expression due to a 'chilling' effect.[15]

The Pegasus software, developed by the Israeli NSO group, infiltrates digital devices and can access and remotely transmit "emails, texts, phone calls, as well as the camera and sound recording capabilities of the device" and can also access its stored data. In 2018, the research laboratory The Citizen Lab discovered that individuals from over 45 countries were suspected to have been targeted by Pegasus. Reports from further investigative efforts alleged that some 50,000 individuals were under surveillance using this spyware. The reports suggested that "nearly 300 of these numbers belonged to Indians, many of whom are senior journalists, doctors, political persons, and even some Court staff".[16]

---

[12] For an overview of regional trends, see Deloitte, 'The Asia Pacific Privacy Guide 2020-2021: Stronger Together' (2020) (accessible: https://www2.deloitte.com/ph/en/pages/risk/articles/asia-pacific-privacy-guide.html) and Graham Greenleaf, 'Advances in South Asian Data Privacy Laws: Sri Lanka, Pakistan and Nepal', (2019) *Privacy Laws & Business International Report*, 22-25 (accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3549055).

[13] Digital Reach, 'Digital Rights in Southeast Asia 2021/2022', (2022) (accessible at: https://digitalreach.asia/event/report-launch-digital-rights-in-southeast-asia-2021-2022/); Smitha Krishna Prasad & Sharngan Aravindakshan (2021) 'Playing catch up – privacy regimes in South Asia', *The International Journal of Human Rights*, 25:1, 79-116, p. 105 (accessible at: https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1773442).

[14] Writ Petition (Crl.) No. 314 of 2021 (India) (2021) (accessible at: https://main.sci.gov.in/pdf/LU/27102021_082008.pdf)

[15] *Id.* at para 21.

[16] *Id.* at paras. 2-3.

In response to media revelations, the government of India has offered cagey explanations, with the country's IT Minister denying illegal use of Pegasus, while not denying actual use of the spyware.[17] This purposeful ambiguity was reflected in the context of the *Manohar* litigation, with the government filing an affidavit containing a blanket denial of the petitioners' allegations without addressing them in any specificity.[18] When afforded opportunities to file a further affidavit, the Solicitor General declined, citing national security concerns as the reason for not revealing further information.[19]

The Supreme Court of India reaffirmed its previous holding in *Puttaswamy*[20] that privacy was 'sacrosanct'[21] and noted that, between the petitioners and the respondent, there was a "broad consensus that unauthorised surveillance/accessing of stored data from the phones and other devices of citizens for reasons other than nation's security would be illegal, objectionable and a matter of concern."[22] The Court also noted that the threat of surveillance impacts how a citizen "decides to exercise his or her rights", and may result in self-censorship, a matter of particular gravity for journalists.[23] The Court further noted the case's significance for the protection of journalistic sources.[24]

The Court found that, in view of the vagueness of the government's affidavit, the petitioners had made out a *prima facie* case for examining their allegations and was quite critical of the government for providing inadequate disclosure in a matter pertaining to fundamental rights.[25] The Court rejected the government's national security rationale for nor revealing any detailed information, noting: "National security cannot be the bugbear that the judiciary shies away from, by virtue of its mere mentioning."[26] Ultimately, the Court declined to order the government to file a further affidavit, considering it had already been granted ample opportunity to do so, and instead ordered the constitution of an Expert Committee headed by a former Supreme Court justice for the purpose of conducting a fact-finding inquiry.[27]

Courts have found cybercrimes legislation to be overbroad where authorities are granted wide-ranging powers to collect or take down certain categories of data without sufficient safeguards. For example, in 2014, the Supreme Court of the Philippines considered the constitutionality of several sections of the 2012 Cybercrime Prevention Act in *Disini et al. v. The Secretary of Justice et al.*[28] The Court upheld many provisions but found several to be unconstitutional because of their overbreadth. For example, section 19 of the Act, which authorised the Department of Justice to restrict or block access to data that was "prima facie found to be in violation of the provisions of this Act" was deemed

[17] The Register, 'India IT minister denies illegal use of NSO Pegasus spyware' (2021) (accessible at: https://www.theregister.com/2021/07/20/ashwini_vaishnaw_bnso_pegasus_denial/).
[18] *Manohar*, n 14 at para 12.
[19] *Id.* at paras. 13-17.
[20] *K.S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012 (2018) (accessible at: https://indiankanoon.org/doc/127517806/).
[21] Manohar, n 14 at para. 32.
[22] *Id.* at para. 52.
[23] *Id.* at para. 39.
[24] *Id.* at paras. 40-41.
[25] *Id.* at paras 46 and 51.
[26] *Id.* at para 49.
[27] *Id.* at paras 54-55.
[28] G.R. No. 203335 (2014) (accessible at: https://lawphil.net/judjuris/juri2014/feb2014/gr_203335_2014.html).

to be inconsistent with constitutional guarantees of freedom of expression and freedom from unreasonable searches and seizures. The Court reasoned that "for an executive officer to seize content alleged to be unprotected without any judicial warrant, it is not enough for him to be of the opinion that such content violates some law, for to do so would make him judge, jury, and executioner all rolled into one".

Another of the provisions of the Act deemed unconstitutional was section 12, which authorised law enforcement authorities to "collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system" with 'traffic data' being defined as "the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities". The section also required service providers to "cooperate and assist law enforcement authorities in the collection or recording" of the traffic data. In finding the provision to be overbroad, the Court reasoned as follows:

> Due cause is also not descriptive of the purpose for which data collection will be used. Will the law enforcement agencies use the traffic data to identify the perpetrator of a cyber attack? Or will it be used to build up a case against an identified suspect? Can the data be used to prevent cybercrimes from happening?
>
> The authority that Section 12 gives law enforcement agencies is too sweeping and lacks restraint. While it says that traffic data collection should not disclose identities or content data, such restraint is but an illusion. Admittedly, nothing can prevent law enforcement agencies holding these data in their hands from looking into the identity of their sender or receiver and what the data contains. This will unnecessarily expose the citizenry to leaked information or, worse, to extortion from certain bad elements in these agencies.
>
> Section 12, of course, limits the collection of traffic data to those "associated with specified communications." But this supposed limitation is no limitation at all since, evidently, it is the law enforcement agencies that would specify the target communications. The power is virtually limitless, enabling law enforcement authorities to engage in [a] "fishing expedition," choosing whatever specified communication they want. This evidently threatens the right of individuals to privacy.

The recognition at the national level of a right to privacy and its extension to the digital realm follows the rapid growth in adoption of data protection legislation around the world since the entry into force of the European Union's General Data Protection Regulations (GDPR) in 2018. The GDPR has set a new standard for the protection of personal data online and has served as a template for numerous other countries' legislation. The California Consumer Privacy Act (CCPA) likewise has sweeping rules regarding consumers' rights to know what personal information is being collected from them, to request deletion of their data, and to opt out of data collection.[29] Because of its application to the technology sector of Silicon Valley, the CCPA has also been lauded for advancing the state of data protection globally.[30]

[29] Forbes, 'California Begins Enforcing Broad Data Privacy Law – Here's What You Should Know' (2020) (accessible at: https://www.forbes.com/sites/siladityaray/2020/07/01/california-begins-enforcing-broad-data-privacy-law---heres-what-you-should-know/?sh=1279e683de5c).
[30] The Guardian, 'California's groundbreaking privacy law takes effect in January. What does it do?' (2019) (accessible at: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do).

Criminalisation of online speech

Cybercrimes legislation often seeks to deal with a wide range of illegal or harmful content that is posted online. This may include incitement to terrorism, hate speech, sexually explicit content such as child pornography, and content which breaches intellectual property rights.[31]

This is often the area in which such legislation conflicts most severely with the right to freedom of expression and the right to information. Any restrictions on these rights must meet the requirements listed under Article 19(3) of the ICCPR: namely that restrictions be provided by law and necessary for one of the exhaustive list of legitimate purposes (to respect the rights or reputations of others or protect national security or of public order, or of public health or morals). In 2011, the UN Special Rapporteur on Freedom of Expression listed the following examples of kinds of expression the restriction of which would fall under these legitimate purposes: (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; (d) defamation; and (e) incitement to discrimination, hostility or violence.[32]

Even legislation that does criminalise these forms of expression needs to be precise, have adequate and effective safeguards against abuse or misuse in order to meet the requirements of legality and necessity. For example, in the case of restrictions on child pornography, the Special Rapporteur noted that the safeguards should include oversight and review by an independent and impartial tribunal or regulatory body.[33] In 2018, the Special Rapporteur stated: "Broadly worded restrictive laws on "extremism", blasphemy, defamation, "offensive" speech, "false news" and "propaganda" often serve as pretexts for demanding that companies suppress legitimate discourse."[34]

Criminalisation of online speech can occur through the application of cybercrime legislation or through the application of non-internet-specific criminal provisions. A 2017 report by the Association for Progressive Communications comparing India, Malaysia, Myanmar, Pakistan and Thailand's laws found:

> All these states either have laws that target cyberspace specifically (along with legal provisions that affect online speech), or they are moving towards such a law. All of these states also utilise offline laws to criminalise and punish online speech. Most of them also utilise multiple legal provisions to target and criminalise a single instance of online speech. They also prescribe harsher punishments for online "offences" than for offline speech.[35]

For more on the criminalisation of online speech, see Module 3 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online.

---

[31] Article 19, 'Freedom of Expression and ICTs' (2018) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf).
[32] United Nationals Special Rapporteur on the Right to Freedom of Opinion and Expression, Frank La Rue, (2011) para 25 (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
[33] *Id.* at para. 71.
[34] United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression, (2018) para 13 (accessible at: https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf.)
[35] Association for Progressive Communications, 'Unshackling expression: A study on laws criminalising expression online in Asia' (2017) at p. 25 (accessible at: https://www.giswatch.org/sites/default/files/giswspecial2017_web.pdf).

Cyberstalking and online harassment

Online harassment is becoming increasingly prevalent with the spread of social media, which can provide especially fertile ground for it. Cyberstalking is undue harassment and intimidation through electronic communications, such as text messages, phone calls or social media posts, and it can severely restrict the enjoyment by the victims of their rights online, particularly if they come from vulnerable and marginalised groups, including women and members of sexual minorities. Research has shown that online harassment is often focused on personal or physical characteristics, with political views, gender, physical appearance and race being among the most common.[36] Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.[37]

A worrying new trend: non-consensual dissemination of intimate images

A particular form of online harassment that has emerged as a concerning new trend is the non-consensual public sharing online of private and sexually explicit images, mostly of women, often by former partners in retaliation for a break-up or other falling out, or for the purposes of extortion, blackmail or humiliation. However, the cybercrimes legislation in only a few countries specifically provides for offences related to non-consensual dissemination of intimate images (NCII), often leaving victims with insufficient recourse against perpetrators due to gaps in legal protection.[38] The Philippines[39] and Singapore[40] are examples of exceptions to this, with both states' having specifically criminalised NCII.

The importance of a name

The non-consensual dissemination of intimate images is often referred to as 'revenge porn'. However, activists and researchers have universally rejected the term as being misleading.[41] Firstly, the word 'revenge' implies that the victim has committed a harm worth seeking revenge for. Secondly, 'porn' conflates the practice with the consensual production of content for mass consumption, which NCII decidedly is not. Thirdly, the term "repackages an age-old harm as a new-fangled digital problem," belying the long history that exists of images of women being

[36] Pew Research Center, 'Online harassment 2017, (2017), (accessible at: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/).
[37] *Id.*
[38] For example, India's legislative regime on NCII has been criticised as being underdeveloped. See for example, Vaishnavi Sharma, 'Understanding Non-Consensual Dissemination of Intimate Images Laws in India with Focus on Intermediary Liability' 14 NUJS L. Rev. 4 (2021) (accessible at: http://nujslawreview.org/wp-content/uploads/2022/03/14.4-Sharma-1.pdf).
[39] *Anti-Photo and Video Voyeurism Act of 2009,* Republic Act No. 9995 at section 4 (accessible at: https://www.lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html).
[40] Penal Code of 1871 (as of 15 June 2022) at section 377BC(1)(a) (accessible at: https://sso.agc.gov.sg/Act/PC1871?ProvIds=pr377BC-#pr377BC-) Prior to the introduction of this offence, certain NCII cases were prosecuted under the now repealed section 509 of the Penal Code which criminalised certain acts against the 'modesty' of women. See for example, *Ang Zhu Ci Joshua v. Public Prosecutor*, [2016] SGHC 143 (2016) (accessible at: https://www.elitigation.sg/gdviewer/s/2016_SGHC_143).
[41] GenderIT, '"Revenge Porn": 5 important reasons why we should not call it by that name' (2019) (accessible at: https://www.genderit.org/articles/5-important-reasons-why-we-should-not-call-it-revenge-porn).

distributed non-consensually across a range of mediums.[42] Lastly, the term oversimplifies the offence by ignoring a range of aggressors and motivations and invoking a moralist reaction against the victim.[43]

Ongoing harassment and attacks on members of the media have also become a particularly worrying trend.

Cyberbullying

It is also worth noting that the crime of cyberbullying, which is the sending of intimidating or threatening messages, often via social media, and which is prevalent among children and young adults. According to the United Nations Children's Fund (UNICEF):

> "[Cyberbullying] can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include:
>
> - spreading lies about or posting embarrassing photos of someone on social media;
> - sending hurtful messages or threats via messaging platforms;
> - impersonating someone and sending mean messages to others on their behalf.
>
> Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint — a record that can prove useful and provide evidence to help stop the abuse."[44]

The scale of the problem is significant and growing. A study by UNICEF and the UN Special Representative of the Secretary-General (SRSG) on Violence against Children found that one in three young people in 30 countries reported being a victim of online bullying.[45]

Cyberbullying Legislation in the Philippines

The Philippines has sought to address cyberbullying among children through the Anti-Bullying Act of 2013.[46] The law requires that primary and elementary schools adopt an anti-bullying policy and creates annual reporting requirements for schools and school boards. Under section 2(d),

---

[42] *Id.*
[43] Association for Progressive Communications, 'Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences' (2017) at p.21 (accessible at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf)).
[44] UNICEF, 'Cyberbullying: What is it and how to stop it' (accessible at: https://www.unicef.org/end-violence/how-to-stop-cyberbullying).
[45] UNICEF, 'UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying' (2019) (accessible at: https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying).
[46] The Republic Act No. 10627 (accessible at: https://lawphil.net/statutes/repacts/ra2013/ra_10627_2013.html).

'bullying' is defined as including: "Cyber-bullying or any bullying done through the use of technology or any electronic means." This is an innovative approach which may be contrasted with the normally overbroad approach taken in some countries of trying to criminalise cyberbullying.

Other violations

The Budapest Convention on Cybercrime defines the following types of cybercrimes:

- Illegal access to a computer system;
- Illegal interception;
- Data interference;
- System interference;
- Misuse of devices;
- Computer-related forgery;
- Computer-related fraud;
- Child pornography;
- Offences related to infringements of copyright and related rights.[47]

Although these definitions date to 2001, much of what constitute cybercrimes today is still covered by these categories and provisions.

TRENDS IN SOUTH AND SOUTHEAST ASIA

South and Southeast Asia have experienced rapid growth in access to the internet in recent years. This increased digitalisation of society has afforded increased opportunities for citizens to exercise their rights to freedom of expression and to information. However, with increasing digitisation also come new security threats and, in turn, new rights concerns raised by many states' approaches to emerging threats.

A 2021 INTERPOL report noted: "Given their position among the fastest growing digital economies in the world, ASEAN [Association of Southeast Asian Nations] member countries have become a prime target for cyberattacks."[48] In response to growing cybersecurity threats, the Association of Southeast Asian Nations has taken certain steps towards multilateral cooperation on cybersecurity matters, notably becoming the first regional organisation to subscribe in principle to the UN's 11 voluntary, non-binding norms of responsible state behaviour in cyberspace,[49] a series of principles

[47] Council of Europe, 'The State of Cybercrime Legislation in Africa – an Overview' at p. 2 (2015) (accessible at: https://rm.coe.int/16806b8a79) at p 3.
[48] INTERPOL, *ASEAN Cyberthreats Assessments 2021* (2021) at p. 13 (accessible at: https://www.interpol.int/en/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf).
[49] Channel Asia, 'How ASEAN is driving global cyber security efforts' (2021) (accessible at: https://www.channelasia.tech/article/691880/how-asean-driving-global-cybersecurity-efforts/).

that were elaborated in a 2015 report by a Group of Governmental Experts[50] and subsequently endorsed in a UN General Assembly resolution.[51]

At the national level, across South and Southeast Asia, governments have been adopting new cybercrimes legislation, often to keep pace and continue to protect against crimes committed online. Every state in South and Southeast Asia, with the exceptions of Cambodia, Myanmar and the Maldives, have adopted some form of cybercrimes legislation.[52] Cambodia, Myanmar and the Maldives are currently in the process of drafting such legislation.[53]

However, cybercrimes legislation is increasingly being used to unjustly regulate internet content as well, including undesirable criticism or dissent. Access Now notes that one of the main concerns about the plethora of laws that are currently being enacted to regulate cybercrimes is that many of them lack clear definitions and are susceptible to being used to over-regulate online content and restrict freedom of expression.[54] This is a growing concern among human rights defenders as many have been subjected to a wave of arrests and convictions in what is an escalating assault on freedom of expression using cybercrime laws. Many of the laws are vague and overbroad and lack clear definitions, leaving them open to arbitrary and subjective interpretations. Some common examples of overbroad provisions are those that criminalise spreading false information or harming national unity.

For example, Bangladesh's Digital Security Act has been widely criticised for its overbroad and vague provisions, which have been used to target critics of the government.[55] For instance, cartoonists and journalists who published cartoons and commentary critical of the government's COVID-19 response have been charged under that law with spreading "propaganda, false or offensive information, and information that could destroy communal harmony and create unrest."[56]

STEPS TO TAKE IN RESPONSE TO ONLINE HARMS

This section lays out practical approaches to dealing with various online harms.

---

[50] UN General Assembly, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174 (2015).
[51] UN General Assembly, 'Developments in the field of information and telecommunications in the context of international security', UN Doc A/RES/70/237 (2015) (accessible at: https://undocs.org/Home/Mobile?FinalSymbol=a%2Fres%2F70%2F237&Language=E&DeviceType=Desktop&LangRequested=False).
[52] United Nations Conference on Trade and Development, 'Cybercrime Legislation Worldwide' (2021) (accessible at: https://unctad.org/page/cybercrime-legislation-worldwide).
[53] *Id.* For a critical analysis of Myanmar's new Draft Cyber Security Legislation, see Centre for Law and Democracy, 'Myanmar: Note on New Draft Cyber Security Law' (2022) (accessible at: https://www.law-democracy.org/live/wp-content/uploads/2022/05/Myanmar.Cyber-Security-Analysis-English-.pdf).
[54] Access Now, 'When "cybercrime" laws gag free expression: stopping the dangerous trend across MENA' (2018) (accessible at: https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/).
[55] See, for example, Human Rights Watch, Meenakshi Ganguly, 'Limiting Free Speech Undermines the Fight Against Covid-19, (2021) (accessible at: https://www.hrw.org/news/2021/02/24/limiting-free-speech-undermines-fight-against-covid-19).
[56] *Id.* See also, Human Rights Watch, 'Bangladesh: Repeal Abusive Law Used in Crackdown on Critics' (2020) (accessible at: https://www.hrw.org/news/2020/07/01/bangladesh-repeal-abusive-law-used-crackdown-critics).

- **Tell the story and engage in advocacy.** While ensuring that the identity of the victim or survivor is fully protected, identify the online harms which were committed and brief the press and start an advocacy campaign. Too often, reporting is limited on online harms, which enables these practices to grow.
- **Consider domestic legal challenges.** Many cybercrimes laws in Asia arguably breach fundamental rights and freedoms, especially in their vagueness and generality. In such cases, recourse to the courts may provide relief, especially in constitutional democracies.
- **Approach UN mechanisms.** In cases where cybercrimes legislation is being used to unjustly violate rights and freedoms, and domestic courts have been unwilling to provide an adequate remedy, impacted individuals or groups may consider whether they can file an individual complaint with a competent international treaty body, such as the UN Human Rights Committee. For residents of states which have not recognised a relevant UN treaty body's jurisdiction over individual complaints, individuals may still seek to raise their concerns through communications to UN special rapporteurs or, in the case of arbitrary detentions under cybersecurity legislation, with the UN Working Group on Arbitrary Detention. (For more on UN Mechanisms, see Module 11 of this course.)
- **Consider obtaining an interdict/injunction or harassment order.** A harassment or protection order can be an inexpensive civil remedy which can be useful in cases where the behaviour may not constitute a crime but may impact negatively on the rights of a person. The order prohibits a person from harassing another person, and breaching it constitutes an offence, which is usually punishable by a fine or a period of imprisonment. Many anti-harassment acts include bullying and cyberstalking. For example, Singapore's Protection from Harassment Act includes certain cybercrimes, such as 'doxxing' (the publication of personal information or images with the intention of harassing or causing violence).[57]
- **Report behaviour to the relevant platform that was used.** Most social media platforms have mechanisms for reporting illegal or unethical behaviour, which may result in content being taken down or action taken against the offending user. It may help to review the relevant platforms' terms of use prior to reporting to identify the most salient term or condition that has been violated.[58]

CONCLUSION

Although the rise of cybercrimes must be addressed, the growing trend of using cybercrimes legislation to clamp down on dissent and free speech is deeply concerning. While the internet is a rapidly evolving space, legislation can and should be designed to include specific protections against online harms both at an individual level, such as cyberstalking, and at a societal level, such as regulating the flow and use of personal data. In doing so, there is a need for countries in Asia to ensure that any initiatives are compliant with international human rights standards, including not

[57] See Singapore Legal Advice, 'Guide to Singapore's Protection from Harassment Act (POHA)' (2022) (accessible at: https://singaporelegaladvice.com/law-articles/singapore-protection-harassment-act/).
[58] Complaints platforms are available:
Facebook: https://www.facebook.com/help/263149623790594;
Instagram: https://help.instagram.com/192435014247952;
Twitter: https://help.twitter.com/en/rules-and-policies/twitter-report-violation#:~:text=Open%20the%20profile%20you'd,the%20issue%20you're%20reporting;
YouTube: https://support.google.com/youtube/answer/2802027?co=GENIE.Platform%3DAndroid&hl=en-GB; and
TikTok: https://support.tiktok.com/en/privacy-safety/report-inappropriate-content-default.

unjustifiably restricting freedom of expression and privacy rights. Social media companies also have a role to play in ensuring that their platforms are not used for the distribution of illegal and harmful content. In addition, governments, internet companies and civil society have a role to play in increasing digital literacy, in particular knowledge of available means to enhance the security of online communications.