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

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes and must be made available under the same "share alike" terms. Full licence terms can be found at https://creativecommons.org/licenses/by-ncsa/4.0/legalcode.

Table of Contents

MODULE 1: KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION 6

INTRODUCTION 6

KEY PRINCIPLES OF INTERNATIONAL LAW 7

Human rights in international law 7

Applying international law in a domestic context 7

THE RIGHT TO FREEDOM OF EXPRESSION UNDER INTERNATIONAL LAW 8

Freedom of expression under international law 8

Freedom of expression online 9

UNITED NATIONS 10

NEW CHALLENGES POSED BY THE RISE IN DIGITAL TECHNOLOGIES 11

CONCLUSION 12

MODULE 2: INTRODUCTION TO DIGITAL RIGHTS 13

INTRODUCTION 13

WHAT ARE DIGITAL RIGHTS? 14

WHAT IS AN INTERNET INTERMEDIARY? 15

THE BORDERLESS ENJOYMENT OF FREEDOM OF EXPRESSION 17

THE RIGHT TO FREEDOM OF EXPRESSION ONLINE 18

CONCLUSION 19

MODULE 3: ACCESS TO THE INTERNET 20

IS THERE A RIGHT TO THE INTERNET UNDER INTERNATIONAL LAW? 20

INTERFERENCES WITH ACCESS TO THE INTERNET 23

WHAT IS AN INTERNET SHUTDOWN? 24

WHAT IS THE BLOCKING AND FILTERING OF CONTENT? 24

WHAT IS NETWORK NEUTRALITY? 25

LIMITATION OF THE RIGHT TO FREEDOM OF EXPRESSION 27

NATIONAL SECURITY AS A GROUND OF JUSTIFICATION 29

INTERMEDIARY LIABILITY 31

CONCLUSION 33

MODULE 4: DATA PRIVACY AND DATA PROTECTION 34

INTRODUCTION 34

THE RIGHT TO PRIVACY 34

DATA PROTECTION 35
'THE RIGHT TO BE FORGOTTEN' 38
ENCRYPTION AND ANONYMITY ON THE INTERNET 41
GOVERNMENT-LED DIGITAL SURVEILLANCE 43
CONCLUSION 46
MODULE 5: DEFAMATION 47
INTRODUCTION 47
WHAT IS DEFAMATION? 48
CRIMINAL DEFAMATION 48
CIVIL DEFAMATION 50
CAN A TRUE STATEMENT BE DEFAMATORY? 50
THE RIGHT TO PROTECTION AGAINST ATTACKS ON REPUTATION 51
WHAT IS THE RIGHT WAY TO DEAL WITH ONLINE DEFAMATION? 51
TYPES OF POTENTIALLY DEFAMATORY STATEMENTS 53
Opinions versus statements of fact 53
Humour 54
Statements of others 54
Remedies and penalties 56
TYPES OF CLAIMS 56
SLAPP suits 56
Insult laws 57
CONCLUSION 58
MODULE 6: HATE SPEECH 59
INTRODUCTION 59
WAS "HATE SPEECH" INTENDED TO INCITE? 60
MUST VIOLENCE OR HATRED ACTUALLY RESULT? 62
THE DANGER OF VAGUENESS 63
ADVOCACY OF GENOCIDE OR HOLOCAUST DENIAL: SPECIAL CASES? 64
DEFAMATION OF RELIGIONS 65
CONCLUSION 66
MODULE 7: CYBERCRIMES 67
INTRODUCTION 67
WHAT IS A CYBERCRIME? 68
Definition 68
Cybercrimes in international law 68
Cybercrimes in domestic law 69

TYPES OF CYBERCRIMES 70
Data privacy violations 70
Criminalisation of online speech 73
Cyberstalking and online harassment 74
Cyberbullying 75
Other violations 76
TRENDS IN SOUTH AND SOUTHEAST ASIA 76
STEPS TO TAKE IN RESPONSE TO ONLINE HARMS 77
CONCLUSION 78
MODULE 8: 'FALSE NEWS', MISINFORMATION AND PROPAGANDA 80
INTRODUCTION 80
WHAT IS 'FALSE NEWS' 81
MISINFORMATION, DISINFORMATION AND MAL-INFORMATION 82
The problem statement 82
Causes of dis- and misinformation 83
How to combat dis- and misinformation 85
STRATEGIES TO ADDRESS "FALSE NEWS" 85
Media and Information Literacy (MIL) Strategies and Campaigns 85
Litigation Where Justifiable Limitations Exist 87
Fact-checking and Social Media Verification 87
PROPAGANDA 89
CONCLUSION 89
MODULE 9: NATIONAL SECURITY 90
INTRODUCTION 90
THE DEROGATION PROCESS UNDER INTERNATIONAL 91
LIMITING MEDIA FREEDOM ON GROUNDS OF NATIONAL SECURITY 91
THE SCOPE OF NATIONAL SECURITY 93
TERRORISM 94
Defining terrorism 94
Terrorism and internet shutdowns 95
PRESCRIBED BY LAW 96
NECESSARY IN A DEMOCRATIC SOCIETY 97
PRIOR RESTRAINT IN NATIONAL SECURITY CASES 98
CONCLUSION 99
MODULE 10: VIOLENCE AGAINST JOURNALISTS 100
INTRODUCTION 100

THE DUTY TO PROVIDE A FAVOURABLE ENVIRONMENT FOR FREEDOM OF EXPRESSION 100
PHYSICAL ATTACKS 101
ONLINE VIOLENCE, SUCH AS ABUSE, TROLLING AND SMEAR CAMPAIGNS 105
PROTECTION OF JOURNALISTIC SOURCES 107
GENDER-BASED VIOLENCE 110
PRACTICAL APPROACHES 113
CONCLUSION 115
MODULE 11: INTRODUCTION TO UN MECHANISMS 116
INTRODUCTION 116
OVERVIEW OF UN MECHANISMS 117
Treaty Bodies 117
The Human Rights Council 118
The Principal Organs of the United Nations 119
RECOURSE UNDER TREATY BODIES 120
Individual Complaints 120
Treaty body reviews 123
RECOURSE UNDER THE SPECIAL PROCEDURES 124
CONCLUSION 124

MODULE 1: KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

- **Human rights have become firmly entrenched in international law since the adoption of the seminal Universal Declaration of Human Rights in 1948.**
- **Since then, international human rights law has become increasingly influential in domestic courts and has set a global standard for the protection of human rights.**
- **Freedom of expression is one right that has benefitted from this trend, but faces novel challenges due to the dramatic changes to the media and information eco-system occasioned by the rise of digital communications technologies.**
- **United Nations mechanisms provide tools for those seeking to challenge violations of freedom of expression.**

INTRODUCTION

Since at least the formation of the United Nations (UN) and the establishment of the modern regime of international human rights law in the wake of World War II, the right to freedom of expression has become universally acknowledged. An example of this universal acknowledgement is found in the case of *Shreya Singhal v. Union of India* from the Supreme Court of India, in which the Court stated:

> The Preamble of the Constitution of India inter alia speaks of liberty of thought, expression, belief, faith and worship. It also says that India is a sovereign democratic republic. It cannot be over emphasized that when it comes to democracy, liberty of thought and expression is a cardinal value that is of paramount significance under our constitutional scheme.[1]

Because the right to freedom of expression is protected in so many treaties and soft law instruments, and widely acknowledged in domestic constitutional guarantees, it has come to be regarded as a principle of customary international law.[2] Nevertheless, today's rapidly evolving world is presenting new and unprecedented threats to the full realisation of the right to freedom of expression for many around the world, especially journalists and the media.

In order for defenders of freedom of expression in South and Southeast Asia to address these new challenges adequately, it is crucial to have a firm understanding of freedom of expression in international law. This Module seeks to provide an overview of the key principles related to freedom

[1] Supreme Court of India, Writ Petition (Criminal) No. 167 (2012) at para. 8 (accessible at https://indiankanoon.org/doc/110813550/) [Emphasis Added].
[2] See article 38 of the Statute of the International Court of Justice (1948) (accessible at https://legal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf) which documents the four recognised sources of international law.

of expression in international law and provide a foundation for understanding how to use these principles in the new digitally-connected world.

KEY PRINCIPLES OF INTERNATIONAL LAW

Human rights in international law

Human rights are inherent to everyone and set out minimum standards for treatment of all people. They are enshrined in both national and international law, and everyone is entitled to enjoy such rights without discrimination. When fully realised, human rights reflect the minimum standards needed to enable people to live with dignity, freedom, equality, justice and peace.

The cornerstones of human rights are that they are considered to be inalienable and therefore cannot be taken away; interconnected and therefore dependant on one another; and indivisible, meaning that they cannot be treated in isolation. Not all rights are absolute; some rights may be subject to certain limitations and restrictions in order to balance competing rights and interests.

Human rights under international law are rooted in the Universal Declaration of Human Rights (UDHR), which was agreed to by the United Nations in 1948 following the end of World War II. The UDHR is not a binding treaty in itself, but countries can be bound by those UDHR principles that have acquired the status of customary international law. Indeed, many of the provisions of the UDHR, including its article 19 guarantee of freedom of expression, are generally considered to reflect customary norms. The UDHR has further been the catalyst to creating other binding legal instruments, most notably the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Together, these three instruments constitute what is known as the International Bill of Rights. Since their adoption, additional thematic treaties have been developed to address certain topics, such as:

- The International Convention on the Elimination of All Forms of Racial Discrimination;
- The Convention on the Elimination of All Forms of Discrimination against Women;
- The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment;
- The Convention on the Rights of the Child;
- The International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families;
- The Convention on the Rights of Persons with Disabilities; and
- The International Convention for the Protection of All Persons from Enforced Disappearance.

Applying international law in a domestic context

International human rights law is binding on states and sets a standard for domestic law to follow. As summarised by the UN Human Rights Committee in relation the rights to freedom of opinion and expression guaranteed in the ICCPR:

> The obligation to respect freedoms of opinion and expression is binding on every party as a whole. All branches of the State (executive, legislative and judicial) and other public or governmental authorities, at whatever level – national, regional or local – are in a position to engage the responsibility of the

> State party. Such responsibility may also be incurred by a State party under some circumstances in respect of acts of semi-State entities. The obligation also requires States parties to ensure that persons are protected from any acts by private persons or entities that would impair the enjoyment of the freedoms of opinion and expression to the extent that these Covenant rights are amenable to application between private persons or entities.[3]

However, the exact way in which international law obligations are implemented domestically can vary from country to country.

The way in which international law applies domestically is largely determined by whether a state applies monist or dualist principles:

- **Monist** states are those where international law is automatically part of the domestic legal framework. However, the exact status of international law — whether above or on par with a state's constitution or domestic law — varies.
- **Dualist** states are those where international treaty obligations only become domestic law once they have been enacted by the legislature. Until this has happened, they are not formally part of the domestic legal system. However, in practice, international law is often still a useful tool for interpreting domestic law, and many courts have developed legislative or doctrinal principles whereby interpretations that are in conformity with international law will be preferred.[4]

States with common law systems are more often dualist, and states with civil law systems are more likely to be monist. However, the issue of how international law is treated by domestic courts is often more nuanced in practice. For example, constitutional or statutory requirements to consider international law in many jurisdictions can blur the idealised categories of 'monist' and 'dualist' systems. Because the application of international law is so varied and complicated, practitioners must evaluate the specific context in a given country to understand how to apply international law and standards most effectively.

THE RIGHT TO FREEDOM OF EXPRESSION UNDER INTERNATIONAL LAW

Freedom of expression under international law

The rights guaranteed by article 19 of the ICCPR comprise three distinct but interrelated rights: the right to hold opinions without interference (freedom of opinion); the right to seek and receive information (access to information); and the right to impart information (freedom of expression).

The UN Human Rights Committee's (UNHRCtte) General Comment No. 34 provides the Committee's authoritative views on the correct interpretation of article 19. In this comment, the Committee notes that the right to freedom of expression includes, for example, political discourse, commentary on one's own affairs and on public affairs, canvassing, discussion of human rights,

---

[3] General Comment No. 34, Article 19: Freedoms of opinion and expression, 12 September 2011, CCPR/G/GC/34 at para. 7 (accessible at: http://undocs.org/ccpr/c/gc/34).
[4] See for example, the Supreme Court of India's judgment in *State Of West Bengal vs Kesoram Industries Ltd. And Ors*, Appeal (civil) 1532 of 1993 (2004) (accessible at: https://indiankanoon.org/doc/879535/).

journalism, cultural and artistic expression, teaching, and religious discourse.[5] It also embraces expression that may be regarded by some as deeply offensive.[6] The right covers communications that are both verbal and non-verbal, and all modes of communication, including audio-visual, electronic and internet-based.[7]

Under 19(3) of the ICCPR, the right to freedom of expression may legitimately be subject to certain restrictions. A three-part test is used to assess whether such a restriction is justified: (i) the restriction must be provided for in law; (ii) it must pursue a legitimate aim; and (iii) it must be necessary to protect a legitimate aim.[8] The ICCPR provides an exhaustive list of legitimate aims, namely the rights or reputations of others or national security, public order, public health or morals. A similar test applies to the right to freedom of expression as guaranteed under other legal instruments.

In relation to the first step of this tripartite test, the requirement that a restriction be "provided by law", the UNHRCtte provides the following guidance:

> For the purposes of paragraph 3, a norm, to be characterized as a "law", must 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. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.[9]

The requirement that a restriction of freedom of expression be 'necessary' for a legitimate purpose implies that the restriction is proportionate. The UNHRCtte notes the following:

> Restrictions must not be overbroad. The Committee observed in general comment No. 27 that "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".[10]

Freedom of expression online

Article 19(2) of the ICCPR stipulates that the right to freedom of expression applies regardless of frontiers and through any media of one's choice. General Comment No. 34 further confirms that article 19(2) protects digital modes of communication.[11]

---

[5] UNHRCtte, General Comment No. 34, above n 3 at para 11.
[6] *Id.* at para 11. For further discussion on this, see Nani Jansen Reventlow, 'The right to 'offend, shock or disturb', or the importance of protecting unpleasant speech' in Perspectives on harmful speech online: A collection of essays, Berkman Klein Center for Internet & Society, 2016 at pp 7-9 (accessible at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746096).
[7] General Comment No. 34, above n 3 at para 12.
[8] For a fuller discussion on how freedom of expression may be legitimately limited, see the training manual published by Media Defence on the principles of freedom of expression under international law: Richard Carver, 'Training manual on international and comparative media and freedom of expression law' at pp 14-16 (2018) accessible at: https://www.academia.edu/27961726/Training_manual_on_international_and_comparative_media_and_freedom_of_expression_law).
[9] General Comment No. 34, above n 3 at para 25.
[10] *Id.* at para 34.
[11] *Id.* at para 12.

In a 2016 resolution, the UN Human Rights Council (UNHRC) affirmed:[12]

> "[T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

While freedom of expression is protected by a considerable body of treaty law, it can also be regarded as a principle of customary international law, as evidenced, *inter alia*, by how frequently the principle is enunciated in treaties, other soft law instruments and constitutional guarantees.[13] Many human rights treaties, including those dedicated to the protection of the rights of specific groups — such as women, children and people with disabilities — also make explicit mention of freedom of expression.[14]

Freedom of expression in the digital age

In recent years, freedom of expression has been under attack in a variety of new and challenging ways. First, the rise of social media and new media platforms has in many countries decimated the revenue model for independent media, leaving many media houses financially strapped and unable to consistently play their crucial role of holding power to account. Secondly, the rise of the internet has upended the traditional information eco-system in various ways. This has resulted in a backlash from governments seeking to regulate growing cybercrimes and a flood of misinformation, often to the detriment of freedom of expression and legitimate dissent.[15] Many states in South and Southeast Asia have been following this unfortunate trend of reacting to novel digital challenges through new laws and policies that are inconsistent with international standards.[16]

UNITED NATIONS

The United Nations enshrined the right to freedom of expression in international law in 1948 with the Universal Declaration of Human Rights. Article 19 states: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek,

[12] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/32/L.20 (2016) at para 1 (accessible at: https://digitallibrary.un.org/record/845728?ln=en).
[13] Carver above at n 8 at p. 5.
[14] *Id.* at p 5.
[15] For more see Washington Post, 'There's a worrying rise in journalists being arrested for 'fake news' around the world' (2019) (accessible at: https://www.washingtonpost.com/world/2019/12/12/theres-worrying-rise-journalists-being-arrested-fake-news-around-world/) and Freedom House, 'The Rise of Digital Authoritarianism: Fake news, data collection and the challenge to democracy' (2018) (accessible at: https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy).
[16] 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). For a more recent overview of jurisprudence from South Asia, see Divya Srinivasan and Gayatri Khandhadai, Association for Progressive Communications, 'Jurisprudence Shaping Digital Rights in South Asia' (2020) (accessible at: https://www.apc.org/sites/default/files/Jurisprudence_Shaping_Digital_Rights_in_South_Asia_Dec_10_3.pdf).

receive and impart information and ideas through any media and regardless of frontiers." This was the foundation of what later became article 19 of the ICCPR.

The ICCPR is not the only treaty in the United Nations framework to guarantee the right to freedom of expression. For instance:

- Article 15(3) of the ICESCR specifically refers to the freedom required for scientific research and creative activity, providing: "The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity."
- Articles 12 and 13 of the UN Convention on the Rights of the Child (CRC) contain extensive protections relating to the right to freedom of expression enjoyed by children.
- Article 21 of the United Nations Convention on the Rights of Persons with Disabilities (CRPD) contains extensive protections relating to freedom of expression and access to information.

It is therefore clear that the right to freedom of expression is firmly entrenched within the United Nations system, both as an important right on its own, as well as a crucial enabling right. For example, General Comment No. 25, in the context of the right to participate in public affairs, voting rights and the right of equal access to public service, noted:

> "Citizens can also take part in the conduct of public affairs by exerting influence through public debate and dialogue with their representatives or through their capacity to organize themselves. This participation is supported by ensuring freedom of expression, assembly and association."[17]

South and Southeast Asia have only rather limited regional human rights systems and no human rights court. However, the UN human rights system has various means for protecting human rights, including freedom of expression, globally, including in these regions. For more on the UN mechanisms, see Module 11 of this course.

NEW CHALLENGES POSED BY THE RISE IN DIGITAL TECHNOLOGIES

The rise of digital technologies poses a number of novel challenges for human rights protection. After providing an overview of the meaning of digital rights in Module 2, this course covers some of the most pressing issues in promoting human rights protection in the digital age:

- What obligations do states have in respect of ensuring access to the internet and guaranteeing 'net neutrality'? (Module 3)
- What are the international standards regarding privacy and data protection and what is meant by the 'right to be forgotten'? (Module 4)
- How should the law of defamation be applied to digital communications? (Module 5)
- What are the international standards on regulating hate speech and what challenges does the rapid spread of information on social media platforms pose for this issue? (Module 6)
- What human rights challenges have accompanied the growth of cybercrimes and the often heavy-handed reaction of governments to this problem (Module 7)

[17] UNHRCtte General Comment No. 25 at para 8 (1996) (accessible at: https://undocs.org/Home/Mobile?FinalSymbol=CCPR%2FC%2F21%2FRev.1%2FAdd.7&Language=E&DeviceType=Desktop&LangRequested=False).

- How should the issue of misinformation and disinformation be addressed in a rights-compliant way? (Module 8)
- To what extent is it legitimate to restriction freedom of expression so as to protect national security? (Module 9)
- What are the international standards on the protection of journalists and what novel challenges exist for them in the digital age (Module 10)
- What recourse do United Nations mechanisms provide for state abuses of human rights? (Module 11)

CONCLUSION

The right to freedom of expression is firmly established in international human rights law. Although digital technologies have amplified our ability to express ourselves, their impact on freedom of expression has also raised novel challenges, with particular consequences for journalists and the media. Rather than being eclipsed by these developments, international standards on freedom of expression have been evolving to address new challenges posed by new communications technologies. As a result, international human rights law plays as important a role as ever in ensuring that the right to freedom of expression is respected, protected and fulfilled, giving individuals a powerful tool to advance their rights.

MODULE 2: INTRODUCTION TO DIGITAL RIGHTS

- **Digital rights — which include the right to freedom of expression, privacy and access to information — are the same fundamental human rights as those enjoyed offline but adapted to a new age of technology.**
- **In understanding digital rights, it is important to understand the role of internet intermediaries, a range of actors who enable access to and use of the internet and whose actions play a critical role in protecting or undermining freedom of speech and associated digital rights online.**
- **Freedom of expression online is uniquely powerful because of its borderless nature, but it has created new legal challenges and consequences, such as the growth in dis- and misinformation.**
- **It is crucial that human rights defenders engage with the new challenges posed online and act to protect and promote digital rights in the rapidly evolving online world.**

INTRODUCTION

Digital rights are human rights in the digital realm. The term 'digital rights' speaks to questions around how the same rights that have always been fundamental to all humans — such as freedom of expression, privacy and access to information — are exercised and protected in the era of the internet, social media and technology.

There is a tension between human rights and freedoms, and the rise in restrictions on access to and use of online spaces, which is continuing with increased political polarisation and the growing powers of non-state actors. Protecting and developing online spaces where human rights can be respected and promoted requires effective responses to oppressive regulations, and innovative solutions.

Additionally, understanding digital rights is crucial to being able to protect fundamental human rights online, as very little of our lives today is immune from the forces of technology and the internet that have reshaped how humans communicate, participate and behave. Digital rights are the rights that apply in these spaces, including the particular nuances which come with the application of human rights online.

This module seeks to provide an overview of digital rights and trends affecting freedom of expression online in South and Southeast Asia.

WHAT ARE DIGITAL RIGHTS?

It is now firmly established that the same rights that people have offline should also be protected online, in particular the right to freedom of expression. As stipulated in article 19(2) of the International Covenant on Civil and Political Rights (ICCPR), the right to freedom of expression applies regardless of frontiers and through any media of one's choice.

However, how established principles of freedom of expression should be applied to online content and communications is in many ways still being determined. For example, do bloggers and citizen journalists count as journalists and should they be afforded the same protections with regards to freedom of expression? How should states regulate the re-tweeting or resharing of hate speech as compared to the author of it? What about regulations for defamatory statements from anonymous accounts? These challenges are actively being grappled with by policymakers and courts around the world.

Examples of digital rights issues

To give an idea of the range and complexity of the issues included in the umbrella term 'digital rights,' here are some examples:

- **Access to the internet.** The right to access the internet is not explicitly recognised in human rights treaties, the main ones of which were elaborated prior to the internet's becoming widespread in usage. However, there has been a growing recognition in recent years that states are required to take progressive steps to promote universal access to the internet.[18]
- **Interferences with access to the internet.** In addition to positive obligations to progressively realise improve access to the internet, states are required to refrain from unjustified restrictions on accessing the internet through internet shutdowns, the disruption of online networks and social media sites, and the blocking and filtering of content.[19] All of these are considered forms of prior restraint on freedom of expression for restricting internet users from expressing themselves through these services and websites before the expression actually occurs. International law allows very limited space for such extreme restrictions on freedom of expression.

---

[18] Juan Carlos Lara, 'Internet access and economic, social and cultural rights', Association for Progressive Communications (September 2015) at p 10-11 (accessible at: https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf). The 2019 Report of the UN Secretary-General's High level panel on Digital Cooperation noted that "universal human rights apply equally online as offline – freedom of expression and assembly, for example, are no less important in cyberspace than in cyberspace than in the town square" at p 16 (accessible at: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf). In *Delfi v Estonia*, Application no. 64569/09 (2015) the Grand Chamber of the European Court of Human Rights held that the internet provided an unprecedented platform for the exercise of the right to freedom of expression (accessible at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2264569/09%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-155105%22]}).

[19] See Module 3 of this course for more details.

- **The freedom to choose among information sources.** The 2017 Report of the UN Special Rapporteur on freedom of expression notes that in the digital age the freedom to choose among information sources is meaningful only when internet content and applications of all kinds are transmitted without undue discrimination or interference by non-state actors, including providers.[20] This concept is known as network neutrality, the principle that all internet data should be treated equally without undue interference.[21] In Asia, there has been significant debate about access to zero-rated content, which is applications or websites the usage of which a mobile operator does not count towards a user's monthly data allotment, rendering it 'free'. This is a practice commonly used by social media companies. Although some of these companies have touted zero-rating schemes as a means of providing access to the internet for people who might not otherwise have been able to afford it, in practice they can lead to unfair competition and can distort users' perceptions by only allowing access to particular sites. India is among the jurisdictions to have taken effective action against zero-rating, effectively banning the practice.[22]
- **The right to privacy.** Exercising privacy online is increasingly difficult in a world in which we leave a digital footprint with every action we take online. While data protection laws are on the rise across the world, including Asia, they are of widely varying degrees of comprehensiveness and effectiveness, and often offer insufficient protection against state surveillance activities.[23] Government-driven mass surveillance is on the rise as a result of the development of technology that enables the interception of communications in a variety of new ways, such as biometric data collection and facial recognition technology.[24]

WHAT IS AN INTERNET INTERMEDIARY?

An internet intermediary is an entity which provides services that enable people to use the internet, falling into two categories: (i) conduits, which are technical providers of internet access or transmission services; and (ii) service providers, such as hosts, providers of

[20] UN Special Rapporteur on Freedom of Expression, Report A/HRC/38/35 on the Role of Digital Access Providers at para.\ 23 (2017) (accessible at: https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2017ReporttoHRC.aspx).
[21] For more on net neutrality, see Module 3 of this course and pp 2-9 of Module 5 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online (accessible at: https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-5-trends-in-censorship-by-private-actors/.
[22] BBC, 'India Adopts "World's Strongest" Net Neutrality Norms' (2018), (accessible at: https://www.bbc.com/news/world-asia-india-44796436). See also Module 3 for further details on India's response to zero-rating schemes.
[23] 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). For more information on data protection, see Module 4 of this course.
[24] For more, see page 11 of Module 1 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online (accessible at: https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-1-general-overview-of-trends-in-digital-rights-globally-and-expected-developments/).

content services, such as online platforms (e.g. social media websites), caching providers and storage services.[25]

Examples of internet intermediaries are:

- Network operators, such as Airtel, Globe and Axiata.
- Network infrastructure providers, such as Cisco, Huawei, Ericsson and ZTE.
- Internet access providers, such as MyKRIS, WorldTel and PTCL.
- Communications service providers, such as Telenor, Metfone and SLT-Telecom.
- Social networks, such as Facebook, Twitter and LinkedIn.

One of the most challenging questions relating to internet intermediaries is whether they constitute publishers in the traditional sense of the word. Is an Internet Service Provider (ISP) or even social media platform liable for the content it hosts on behalf of others? Courts have generally found that an ISP does not 'publish' any more than the supplier of newsprint or the manufacturer of broadcasting equipment. As pointed out by the UN Special Rapporteur on Freedom of Expression in 2011:

> "Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law."[26]

Some countries in South and Southeast Asia, such as the Philippines,[27] have laws providing for the limitation of intermediary liability, to help protect themselves from liability even in cases where such legislation does not exist, intermediaries often develop terms and conditions that specify their responsibilities and those of their customers. Other countries in South and Southeast Asia have laws that explicitly make intermediaries liable for their actions regarding content posted using their services.[28]

Additionally, internet intermediaries are increasingly being used by states to police the internet through direct requests to take down content or interfere with internet access, decisions which are often made outside of formal legal and regulatory frameworks and lack transparency and public scrutiny. Even where such actions are authorised under domestic law, often the legislation used is worded in an overly broad manner, giving authorities

---

[25] Association for Progressive Communications, 'Frequently asked questions on internet intermediary liability' (2014) (accessible at: https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-internetintermed).
[26] OHCHR, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2011) (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
[27] See Republic Act No. 8792, June 14, 2000, section 30 (accessible at: https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/2/3888) .
[28] See, for example, Joint Letter of Access Now and 24 other organisations, 'Indonesia: repeal law that imposes harsh intermediary liabilities, risks curtailing expression' (2021) (accessible at: https://www.accessnow.org/indonesia-intermediary-liabilities/).

significant discretion to order content removed on vaguely defined or impermissible grounds. For example, under section 37 of The Prevention of Electronic Crimes Act 2016,[29] the Pakistan Telecommunication Authority is granted "the power to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act."

THE BORDERLESS ENJOYMENT OF FREEDOM OF EXPRESSION

One particular strength of freedom of expression online presents is that the right is able to be enjoyed regardless of physical borders. People are able to speak, share ideas, coordinate and mobilise across the globe on a significant and unprecedented scale.

The internet as a tool for change: the case of Myanmar and the Milk Tea Alliance

Following the 2021 *coup d'état* that led to a military regime taking control of Myanmar's government, activists in Taipei, Bangkok, Melbourne and Hong Kong heeded a call by pro-democracy campaigners in Myanmar and took to the street carrying #MilkTeaAlliance signs.[30] The Milk Tea Alliance online movement for democracy and human rights first emerged in Hong Kong, Taiwan and Thailand, and is an allusion to a shared love for variations of milk tea in those countries, and the hashtag was used to protest online attacks from Chinese nationalists.[31]

Before the internet, this would have been next to impossible. The borderless nature of the internet can lead to international pressure being put on states for rights violations, global campaigns being developed and supported, and a rigorous exchange of ideas being fostered.

However, the internet also gives rise to particular challenges. Through the internet, the ability to publish immediately and reach an expansive audience can create difficulties from a legal perspective, such as establishing the true identity of an online speaker, establishing founding jurisdiction for a legal claim, or achieving accountability for wrongdoing that has spread rapidly online, such as the non-consensual dissemination of intimate images.

Moreover, once content has been published online it can often be very difficult to remove it. In the 2021 case of *T.V. Today Network Limited vs The Cognate & Ors*[32], the New Delhi

[29] Act No. XL of 2016 (accessible at: http://nasirlawsite.com/laws/peca1.htm).
[30] Fanny Potkin and Patpicha Tanakasempipat, Reuters, "'Milk Tea Alliance" activists across Asia hold rallies against Myanmar coup' (2021) (accessible at: https://www.reuters.com/article/us-myanmar-protests-asia-idUSKCN2AS0HP).
[31] *Id.*
[32] Delhi High Court, CS(OS) 246/2021 (2021) (accessible at: https://indiankanoon.org/doc/72053412/)

High Court ordered the deletion of an infographic that had been shared on Twitter, Facebook and Instagram and that was determined to be defamatory. This particular order was worded broadly, and the defendants were also ordered to block related posts on "other social media or any other website on the internet, in print or electronically or other media".[33] However, the viral nature of social media raises questions about the effectiveness of such remedies, particularly where they are broadly worded. The deletion of a tweet on Twitter does not necessarily remove it from all platforms, as there are other ways in which the content may have been distributed that are not addressed by the deletion (such as retweets in which persons added a comment of their own),[34] and third parties responsible for such posts may not be party to the litigation and thus not bound to remove content they have disseminated. This is a particular challenge to finding effective remedies to claims of defamation, hate speech, or the right to be forgotten.

THE RIGHT TO FREEDOM OF EXPRESSION ONLINE

International law is clear that the right to freedom of expression applies online just as it does offline, though there are challenges in implementing this principle in practice. For example, article 19(2) of the ICCPR is explicit that the right to freedom of expression applies "regardless of frontiers," and the United Nations Human Rights Committee (UNHRCttee) General Comment No. 34 further clarifies that this includes internet-based modes of communication.[35]

Challenges to freedom of expression online

Some examples of the new challenges to exercising freedom of expression online include:

- The blocking, filtering, and removal of content, often executed by internet intermediaries on behalf of government outside of regulatory or legislative provisions or pursuant to expansive and vague legislation, and with little transparency or accountability.
- Online content regulation through overly broad and vague cybercrimes legislation which, although ostensibly intending to counter genuinely criminal activity online, such as child pornography, is often misused by governments to stifle criticism and free speech.[36]
- The rapid growth in misinformation and disinformation on online platforms leading to a backlash from states, which react with 'fake news' regulations that often unjustifiably restrict freedom of expression.[37]

[33] *Id.* at para. 27.
[34] ALT Advisory, Avani Singh, 'Social media and defamation online: Guidance from Manuel v EFF', (2019) (accessible at: https://altadvisory.africa/2019/05/31/social-media-and-defamation-online-guidance-from-manuel-v-eff/).
[35] UN Human Rights Council, 'General Comment no. 34 at para. 12 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[36] For more see Module 7 in this series from Media Defence on 'Cybercrimes.'
[37] For more see Module 8 in this series from Media Defence on 'False news, misinformation and propaganda'.

- Defining and protecting journalists and the media in an environment now saturated with bloggers and social media writers, and defending them from online harassment, particularly women who are disproportionately subject to online attacks.
- Enabling free, full and socially relevant access to the internet, including overcoming the challenges of unaffordability while preventing the distortion that can be created by zero-rating.[38]
- Tackling the spread of hate speech on online platforms without placing undue responsibility on private actors to proactively limit content on their platforms.
- Protecting the public from invasive uses of private data and protecting anonymous communications, while simultaneously enabling accountability for illegal behaviour online.

CONCLUSION

Digital rights is a relatively new and dynamic field. Protecting digital rights involves a host of new actors that did not exist previously, such as internet intermediaries. The internet is an incredibly powerful tool for social progress and the fuller realisation of human rights, but it also gives rise to particular challenges. Nevertheless, international law is clear that the same rights that apply offline apply online, and while those challenges might be immense, the benefits of getting it right — a free and fair internet which is accessible to all — are too important not to take digital rights seriously.

[38] For more see Module 3 in this series from Media Defence on 'Access to the internet'.

MODULE 3: ACCESS TO THE INTERNET

- **An obligation on States to progressively promote access to the internet is emerging under international law, in recognition of the fact that access to the internet enables freedom of expression and a variety of other fundamental rights.**

- **Practices such as internet shutdowns and blocking and filtering of content are severe restrictions on the right to freedom of expression which often do not constitute justifiable limitations.**

- **National security is frequently relied upon as the justification for an interference with access to the internet, as well as other interferences with the right to freedom of expression. While national security is listed as one of the legitimate aims for restrictions on the right to freedom of expression in appropriate circumstances, it is often used by states to quell dissent and cover up state abuses.**

- **'Net neutrality' refers to the principle that all internet data should be treated equally without discrimination based on the device, content, author, origin and/or destination of the content, service or application.**

- **Intermediary liability occurs where technological intermediaries, such as internet service providers (ISPs) and websites, may be held legally liable for unlawful or harmful content created by users of those services. Such liability has a chilling effect on freedom of expression online.**

IS THERE A RIGHT TO THE INTERNET UNDER INTERNATIONAL LAW?

Not surprisingly, no human rights treaty explicitly recognising a right to access the internet, given that the main such treaties were developed before internet usage became widespread. However, it is increasingly being recognised that the internet is now central to the exercise of the right to freedom of expression, given that it is the dominant means for disseminating information and ideas, whether this involves giving voice to one's views or accessing information. As such, there is a growing body of authoritative statements to the effect that states are under an obligation to take progressive steps to ensure universal access to the internet.[39]

[39] Juan Carlos Lara, 'Internet access and economic, social and cultural rights', Association for Progressive Communications (September 2015) at p 10-11 (accessible at: https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf). The 2019 Report of the UN Secretary-General's High level panel on Digital Cooperation noted that "universal human rights apply equally online as offline – freedom of expression and assembly, for example, are no less important in cyberspace than in cyberspace than in the town square" at p 16 (accessible at: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf). In *Delfi v Estonia* the European Court of Human Rights held that the internet provided an unprecedented platform for the exercise of the right to freedom of expression (accessible at: https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/).

It is important to understand the nature of this right, as it is being recognised. It is more along the line of certain other economic and social rights, like the right to education, which is recognised by States "with a view to achieving the full realization" over time, rather than immediately.[40] In this regard, it differs significantly from civil and political rights, which states are expected to respect immediately. However, the progressive development of rights does not mean they are inconsequential. Rather, it means that states are required to devote sufficient attention and resources towards achieving these goals.

Although it may seem anomalous to consider access to a certain technology as a right – after all, no right to access broadcasting or the print media has ever been recognised – but the internet is simply not analogous to these other technologies. As important as they were, they do not begin to match the importance of the internet in daily life, and in particular as an expressive medium. Only a tiny fraction of the world's people have ever had a chance to express themselves through the print or broadcast media, whereas this is not the case at all with the internet. It is also relevant to note that Worldwide surveys show a single predominant attitude towards access to the internet: that it should be recognised as a right.[41]

It should also be noted that there are arguments against recognising a right of access to the internet. Some may claim that this is simply not analogous to other human rights or that expanding the scope of rights undermines the high regard placed on a smaller number of core rights. And states have proven somewhat reluctant to recognise this right, given the important implications for them, including in terms of spending. At the same time, the direction here is reasonably clear.

There is also increasing recognition of access to the internet being indispensable to the enjoyment of an array of fundamental rights. The corollary is that those without access to the internet are deprived of the full enjoyment of those rights, which, in many instances, can exacerbate already existing socio-economic divisions. For instance, a lack of access to the internet can impede an individual's ability to obtain key information, facilitate trade, search for jobs, or consume goods and services.

Access entails the technological ability to make use of the internet in a manner that is affordable, safe, secure, effective and meaningful. In 2003, UNESCO was among the first international bodies to call on states to take steps to realise a right of access to the internet. In this regard, it stated that:[42]

> "Member States and international organizations should promote access to the Internet as a service of public interest through the adoption of appropriate policies in order to enhance the process of empowering citizenship and civil society, and by encouraging proper implementation

[40] Article 13, International Covenant on Economic, Social and Cultural Rights, adopted 16 December 1966, in force 3 January 1976 (accessible at: https://www.ohchr.org/sites/default/files/cescr.pdf).
[41] The Internet Society, 'Global Internet User Survey 2012' (2012) (accessible at: https://wayback.archive-it.org/9367/20170907075228/https://www.internetsociety.org/sites/default/files/rep-GIUS2012global-201211-en.pdf).
[42] UNESCO, 'Recommendation concerning the promotion and use of multilingualism and universal access to cyberspace' at paras 7 and 15 (accessible at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf).

> of, and support to, such policies in developing countries, with due consideration of the needs of rural communities.
>
> …
>
> Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation."

In 2012, the United Nations Human Rights Council (UNHRC) passed an important resolution that "[called] upon all States to facilitate access to the Internet and international cooperation aimed at the development of media and information communications facilities in all countries".[43]

This has been expanded upon in the United Nation's Sustainable Development Goals (SDGs), which recognise that "[t]he spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies".[44] The SDGs further call on states to enhance the use of information and communication technologies (ICTs) and other enabling technologies to promote the empowerment of women,[45] and to strive to provide universal and affordable access to the internet in least developed countries by 2020.[46]

The 2016 UN Resolution on the Internet, adopted by the UN Human Rights Council, recognises that the internet can accelerate progress towards development, including in achieving the SDGs, and affirms the importance of applying a rights-based approach in providing and expanding access to the internet.[47] Notably, it affirms the importance of applying a comprehensive rights-based approach in providing and in expanding access to the internet,[48] and calls on states to consider formulating and adopting national internet-related public policies with the objective of universal access and the enjoyment of human rights at their core.[49]

In successive Joint Declarations, the special international mandates on freedom of expression at the UN, OSCE, OAS and African Commission have made it clear that they view the right to freedom of expression as including an obligation on states to promote universal access to the internet. For

---

[43] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/20/L.13, 29 June 2012 at para 2 (accessible at: https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc). This was expanded upon further the following year in UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/Res/26/13, 14 July 2014 (accessible at: https://hrlibrary.umn.edu/hrcouncil_res26-13.pdf).

[44] UNGA, 'Transforming our world: The 2030 agenda for sustainable development', A/Res/70/1, 21 October 2015 at para 15 (accessible at https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E).

[45] *Id.* at goal 5(b) at p 18.

[46] *Id.* at goal 9(c) at p21.

[47] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/Res/32/13, 18 July 2016 at para 2 (accessible at: https://www.refworld.org/docid/57e916464.html).

[48] *Id.* at para 5.

[49] *Id.* at para 12.

example, in their 2011 Joint Declaration on Freedom of Expression and the Internet, they stated: "Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet."[50]

In *Kalda v Estonia*, the European Court of Human Rights (ECtHR) held that the applicant's right to freedom of expression had been violated through a prison's refusal to grant him access to internet websites containing legal information, as this had breached his right to receive information.[51] The ECtHR noted that when a state is willing to allow prisoners access to the internet, as with the case in question, it had to give reasons for refusing access to specific sites.[52]

In addition to these international developments, several countries – including Greece, Estonia, Finland, Spain, Costa Rica and France – have asserted or recognised some right of access in their constitutions, legal codes, or judicial rulings.

Notwithstanding whether the internet is seen as a self-standing right or an enabling tool to facilitate the realisation of other rights, the groundwork has firmly been laid for the need to realise universal access to the internet. States are concomitantly required to take steps to achieve universal access. However, in reality, universal access to the internet is far from being realised. This is due to a confluence of factors, including a lack of political will to make this a priority, inadequate locally-relevant content, insufficient levels of digital literacy, and challenges in providing last mile access in many contexts.

INTERFERENCES WITH ACCESS TO THE INTERNET

Some of the ways in which access to the internet is interfered with are through internet shutdowns, the disruption of online networks and social media sites, and the blocking and filtering of content. Such interferences represent severe restrictions on the enjoyment of the right to freedom of expression, as well as the enjoyment of a range of other rights and services (including mobile banking, online trade and the ability to access government services via the internet).

The act of disrupting or blocking access to internet services and websites amounts to a form of prior restraint. Prior restraints are State actions that prohibit speech or other forms of expression before they can take place.[53] Due to the profound chilling effect prior restraint can have on the exercise of the right to freedom of expression, the International Covenant on Civil and Political Rights (ICCPR) has been interpreted as prohibiting most forms of prior restraint on speech.[54] The American

---

[50] Adopted 1 June 2011, para. 6(a) (accessible at: http://www.law-democracy.org/wp-content/uploads/2011/06/11.06.Joint-Declaration.Internet.pdf).

[51] Application No. 17429, 19 January 2016 (accessible at: https://hudoc.echr.coe.int/eng?i=001-160270).

[52] *Id.* at para 53. In the subsequent decision of *Jankovskis v Lithuania*, Application No. 21575/08, 17 January 2017 (accessible at: https://hudoc.echr.coe.int/eng?i=001-170354), also in relation to a prisoner who had been refused access to a website containing education-related information, the ECtHR again upheld the applicant's claim of a violation of the right to freedom of expression.

[53] Council of Europe, 'Prior Restrains and Freedom Of Expression: The Necessity of Embedding Procedural Safeguards in Domestic System' (May 2018), (accessible at: https://rm.coe.int/factsheet-prior-restraints-rev25may2018/16808ae88c).

[54] See, for example,the *travaux préparatoires* of the ICCPR as elaborated upon in Marc J. Bossuyt, 'Guide to the "Travaux Preparatoires" of the International Covenant on Civil and Political Rights', Martinus Nijhoff (1987) at p 398.

Convention on Human Rights contains a much more explicit prohibition on prior restraints.[55] The justification of any such measure therefore comes with a heavy burden of justification under the three-part test for restrictions on freedom of expression detailed in Module 1.

WHAT IS AN INTERNET SHUTDOWN?

An internet shutdown may be defined as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.[56] In other words, this arises when someone, be it the government or a private sector actor, intentionally disrupts the internet, a telecommunications network or an internet service, arguably to control or curb what people say or do.[57]

In some instances, this may entail there being a total network outage, whereby access to the internet is shutdown in its entirety. This is sometimes also referred to as a 'kill switch'. In other circumstances, this may also arise when access to mobile communications, websites or social media and messaging applications is blocked, throttled or rendered effectively unusable.[58] Shutdowns may affect an entire country, towns or regions within a country, or even multiple countries, and have been seen to range from several hours to several months.[59]

It should be noted that in order to conduct shutdowns governments typically require cooperation from private actors that operate networks or facilitate network traffic.[60] As noted by the United Nations Special Rapporteur (UNSR) on freedom of expression, large-scale attacks on network infrastructure committed by private parties, such as distributed denial-of-service (known as 'DDoS') attacks, may also have shutdown effects.

WHAT IS THE BLOCKING AND FILTERING OF CONTENT?

Although a less drastic measure than a complete internet shutdown, the blocking and filtering of content online can also hinder the full enjoyment of the right to freedom of expression.

Blocking/filtering has been defined as follows:

---

[55] Article 13: "1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. 2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: a. respect for the rights or reputations of others; or b. the protection of national security, public order, or public health or morals."

[56] Access Now, 'What is an internet shutdown?' (accessible at: https://www.accessnow.org/keepiton/?ignorelocale).

[57] *Id.*

[58] Report of the UNSR on Freedom of Expression to the UNGA, A/HRC/35/22, 30 March 2017 (2017 Report of the UNSR on freedom of expression) at para 8 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement).

[59] *Id.*

[60] *Id.*

"[T]he difference between "filtering" and "blocking" is a matter of scale and perspective.

- Filtering is commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful;
- Blocking, by contrast, usually refers to preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist."[61]

For example, internet shutdowns have been common in parts of Myanmar for some time. Since the February 2021 *coup d'état*, the military regime that assumed power has repeatedly resorted to internet shutdowns as one of an array of repressive digital tools. The throttling of internet access has taken different forms in Myanmar, namely national blackouts, regional blackouts and impeding access through speed restrictions and increased data fees.[62] The military regime's imposition of internet shutdowns and other barriers to internet access was condemned in a strongly worded June 2022 joint statement from multiple UN Special Rapporteurs.[63]

Much international attention has focussed on the military regime in Myanmar's use of internet shutdowns due their frequent and protracted nature. However, this is far from the only example of this practice in South and Southeast Asia. In 2021, internet shutdowns were also documented in India, Bangladesh, Indonesia and Pakistan.[64]

WHAT IS NETWORK NEUTRALITY?

Network neutrality — or "net neutrality" — refers to the principle that there should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application.[65] In other words, ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular application, website or service.[66] Discrimination in this regard may relate to affecting information in a way that halts, slows or otherwise tampers with the transfer of any data, except for a legitimate network management purpose, such as easing congestion or blocking spam.[67]

---

[61] ARTICLE 19, 'Freedom of expression unfiltered: How blocking and filtering affect free speech', October 2016 at p 7 (accessible at: https://www.article19.org/data/files/medialibrary/38588/Blocking_and_filtering_final.pdf).

[62] Athan, 'Internet Access Amid Darkness and Lives Amid Threats', May 2022 (accessible: https://progressivevoicemyanmar.org/wp-content/uploads/2022/06/Internet-Shutdown-Athan-May-2022-Eng.pdf).

[63] UN Special Rapporteurs on the situation of human rights in Myanmar, the promotion and protection of freedom of opinion and expression, the right to privacy and the rights to freedom of peaceful assembly and of association, 'Myanmar: UN experts condemn military's "digital dictatorship"' (2022), (accessible at: https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship).

[64] Access Now, 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021', p. 4 (accessible at: https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf).

[65] 2017 Report of the UNSR on freedom of expression above at n 18 at para 23.

[66] Electronic Frontier Foundation, 'Net neutrality' (accessible at: https://www.eff.org/issues/net-neutrality).

[67] American Civil Liberties Union, 'What is net neutrality?' (accessible at: https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality).

The 2017 Report of the UNSR on freedom of expression describes two key ways in which net neutrality may be effected:[68]

- Paid prioritisation schemes — where providers give preferential treatment to certain types of internet traffic over others for payment or other commercial benefit.
- Zero-rating — which is the practice of not charging for internet data associated with accessing a particular application or set of services while such data is charged to access other services or applications.

In various countries in Asia, there has been significant debate about access to zero-rated content, as particularly social networking sites offer some measure of free access to users. On the one hand, the social media companies that promote them argue that zero-rating provides access to people who might not otherwise have been able to access the internet and can serve as a gateway to users to understand the opportunities that the internet can offer. In practice, however, these people often get stuck just accessing the privileged services and, indeed, may even think that these comprise the whole internet. On the other hand, zero-rating leads to unfair competition and can distort users' perceptions by only allowing access to particular sites.[69]

India is among the jurisdictions to have taken action against zero rating, effectively banning it. A 2016 regulation prohibited Internet access providers from offering or charging discriminatory tariffs for data services on the basis of content, with only a limited exception for zero rating for emergency services.[70] The regulation was enacted following an active campaign by digital rights activists in India. This was motivated largely by Facebook's Free Basics programme, which activists criticised for giving free access to only a restricted number of websites pre-selected by Facebook rather than offering broader Internet access for the poor.[71] India has since maintained its zero-rating ban in updated net neutrality rules.[72]

---

[68] 2017 Report of the UNSR on freedom of expression above n 18 at paras 24-28.

[69] For an overview of legal treatment of zero-rating schemes globally, see Centre for Law and Democracy's 2022 *amicus curiae* submissions before the Constitutional Supreme Court in the proceeding of D-14516 on Ley 1450 de 2011, paras. 101-112 (accessible at: https://www.law-democracy.org/live/wp-content/uploads/2022/02/Colombia.Zero-Rating-Brief.CLD_.final_.pdf).

[70] Telecom Regulatory Authority of India, Notification No. 2 of 2016, Prohibition of Discriminatory Tariffs for Data Services Regulations (2016) (accessible at: https://trai.gov.in/sites/default/files/Regulation_Data_Service.pdf).

[71] The Guardian, Aayush Soni, 'India Deals Blow to Facebook in People-Powered "Net Neutrality" Row' (2016), (accessible at: https://www.theguardian.com/technology/2016/feb/08/india-facebook-free-basics-net-neutrality-row and BBC, Soutik Biswas, 'Why is Mark Zuckerberg Angry at Critics in India?' (2015), (accessible at: https://www.bbc.com/news/world-asia-india-35192184).

[72] BBC, 'India Adopts "World's Strongest" Net Neutrality Norms' (2018), (accessible at: https://www.bbc.com/news/world-asia-india-44796436).

LIMITATION OF THE RIGHT TO FREEDOM OF EXPRESSION

In 2016, the UNSR on freedom of expression noted: "The blocking of Internet platforms and the shutting down of telecommunications infrastructure are persistent threats, for even if they are premised on national security or public order, they tend to block the communications of often millions of individuals".[73] This imposes an obvious restriction on the right to freedom of expression, and may further limit a range of other rights.

The 2011 Joint Declaration on Freedom of Expression and the Internet highlights the egregious nature that these limitations can cause:[74]

> "(a) Mandatory blocking of entire websites, (IP) [internet protocol] addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.
>
> (b) Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.
>
> (c) Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering."

Internet and telecommunications shutdowns that involve measures to intentionally prevent or disrupt access to or dissemination of information online are a violation of human rights law.[75] In the 2016 UN Resolution on the Internet, the UN Human Rights Council stated that it "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures".[76]

As set out in General Comment No. 34, adopted by the UN Human Rights Committee:[77]

> "Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with [article 19(3) of the ICCPR]. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with [article 19(3) of the ICCPR]. It is also inconsistent with [article 19(3) of the ICCPR] to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."

---

[73] Report of the UNSR on Freedom of Expression to the UNGA, A/71/373, 6 September 2016 (2016 Report of the UNSR on Freedom of Expression) at para 22 (accessible at: https://www.un.org/ga/search/view_doc.asp?symbol=A/71/373).

[74] 2011 Joint Declaration, above n 12 at para. 3.

[75] *Id.* 12 at para. 6(b).

[76] *Id.* at para 10.

[77] General Comment No. 34 at para 43.

The UNSR on freedom of expression has noted that internet shutdowns are often ordered covertly and without a legal basis, and violate the requirement that restrictions must be provided for in law.[78] Similarly, shutdowns ordered pursuant to vaguely formulated laws and regulations also fail to satisfy the legality requirement.[79] In some countries, this has led to the government enacting new laws to expressly allow for shutdowns to take place.[80]

The UNSR on Freedom of Expression has further noted that network shutdowns invariably fail to meet the standard of necessity,[81] and are generally disproportionate.[82] States frequently seek to justify this on the ground of national security, which is discussed further below. For example, according to the digital rights advocacy group, Access Now, 2021 marked the fourth consecutive year that India was responsible for imposing the highest number of internet shutdowns globally, with 106 shutdown incidents recorded in 2021.[83] According to their research, political instability was the reason for most of India's 2021 shutdowns (80 cases), followed by protests (9 cases) and communal violence (7 cases).[84]

The Supreme Court of India on internet shutdowns

The Supreme Court of India considered legality of an internet shutdown in Kashmir in their 2010 judgment in *Bhasin v. Union of India*.[85] In their reasons, the Court found that a complete shutdown of the internet was a 'drastic measure' that should be "considered by the State only if 'necessary' and 'unavoidable'" and that the State "must assess the existence of an alternate less intrusive remedy."[86] The Court also found that any suspension of the internet must meet the requirement of proportionality and not extend longer than necessary.[87]

[78] 2017 Report of the UNSR on Freedom of Expression, above n 20 at para 9.

[79] *Id.* at para 10.

[80] In India, for example, following the internet reportedly having been shut down more than 40 times during the course of 2017, the Department of Telecommunications issued new rules - the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules - in August 2017 allowing the government to shut down telephone and internet services during a public emergency or for public safety. The government had previously relied on section 144 of the Criminal Code that was aimed at preventing "obstruction, annoyance or injury" to impose internet restrictions. This legal development was met with mixed responses. On the one hand, the 2017 rules meant that government shutdowns could arguably be done in a more organised manner. On the other hand, however, concerns were raised about the lack of definitions for the terms "public emergency" or "public safety", and the potential that these new rules may have for censorship online. See: for instance, http://www.hindustantimes.com/india-news/govt-issues-first-ever-rules-to-carry-out-internet-shutdowns-in-india/story-Drn0MnxJAp58RoZoFI7u4L.html.) In practice, India's use of internet shutdowns increased in subsequent years, and India has been criticised for not implementing the requirement under the 2017 Rules to establish a centralised repository of data on internet shutdowns. See Access Now, 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021', above n 26, p. 7.

[81] 2017 Report of the UNSR on freedom of expression above n 20 at para 14.

[82] *Id.* at para 15.

[83] Access Now, 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021', above n 26, p. 2.

[84] *Id.*, p. 14.

[85] Supreme Court of India, Writ Petition (Civil) No. 1031/2019 (2020) (accessible at: https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf).

[86] *Id.* at para. 99.

[87] *Id.* at paras. 71 & 152(d).

Although the Court adopted a circumspect approach towards internet shutdowns, international standards go even further. Under international human rights law, internet shutdowns are always unjustifiable restrictions of freedom of expression.[88]

In relation to the blocking and filtering of content, there may indeed be circumstances where such measures are justifiable. For example, in relation to websites distributing child pornography. Such measures are still required to meet the three-part test for restrictions, which will need to be assessed on a case-by-case basis.

Similarly, limitations to network neutrality may also be permissible in certain circumstances, for example for legitimate network management purposes. However, as a general principle, there should be no discrimination in the treatment of internet data and traffic, regardless of the device, content, author, origin and/or destination of the content, service or application.[89] Further, internet intermediaries should be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders.[90]

NATIONAL SECURITY AS A GROUND OF JUSTIFICATION

National security is frequently relied upon as a justification for an interference with access to the internet, as well as other restrictions on the right to freedom of expression.[91] While this may, in appropriate circumstances, be legitimate, it also has the potential to be used to quell dissent and cover up state abuses.

The covert nature of many national security laws, policies and practices, as well as the refusal by states to disclose information about national security threats, tends to exacerbate this concern. Furthermore, courts and other institutions have often been unduly deferential to the state in determining what constitutes a national security threat. As has been previously noted:[92]

> "The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."

---

[88] 2017 Report of the UNSR on freedom of expression above n 20, paras 9-14.

[89] 2011 Joint Declaration above n 12 at para. 5(a).

[90] *Id.* at para. 5(b).

[91] For a fuller discussion on national security more broadly see Richard Carver, 'Training Manual on International and Comparative Media and Freedom of Expression Law at p 77-88 (accessible here: https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-international-and-comparative-media-and-freedom-of-expression-law/).

[92] Report of the UNSR on freedom of expression to the UNGA, A/HRC/23/40, 17 April 2013 at para 60 (accessible at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf).

As set out in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (the Johannesburg Principles):[93]

> "(a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.
>
> (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest."

Principle 7 goes on to list a number of circumstances in which the peaceful exercise of the right to freedom of expression should not be considered a threat to national security or subjected to any restrictions or penalties.

Another important principle contained in the Johannesburg Principles is principle 23, which provides: "Expression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country". The measures described above can often give rise to a prior restraint on content, and consequently have a chilling effect on the enjoyment of the right to freedom of expression.

Similarly, counter-terrorism as a purported justification for network shutdowns or other interferences with access to the internet should be treated with extreme caution. As noted in General Comment No. 34, the media plays an important role in informing the public about acts of terrorism, and it should be able to perform its legitimate functions and duties without hindrance.[94] While governments may argue that internet shutdowns are necessary to ban the spread of news about terrorist attacks to prevent panic or copycat attacks, it has instead been found that maintaining connectivity may mitigate public safety impacts and help support public order.[95]

At a minimum, if there is to be a limitation of access to the internet, there should be transparency regarding the laws, policies and practices relied upon, clear definitions of terms such as 'national security' and 'terrorism', and independent and impartial oversight of measures.

---

[93] Principle 2 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, November 1996 (accessible at https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf). The Johannesburg Principles were developed by a group of experts in international law, national security and human rights, convened by ARTICLE 19. It was endorsed by the then UNSR on freedom of expression.

[94] General Comment No. 34 at para 46.

[95] 2017 Report of the UNSR on freedom of expression above n 20 at para 14.

INTERMEDIARY LIABILITY

Intermediary liability is where technological intermediaries, such as ISPs and websites, can be held legally liable for unlawful content disseminated by users of those services.[96] This can arise in various circumstances, including copyright infringements, digital piracy, trademark disputes, network management, spamming and phishing, "cybercrime", defamation, hate speech, child pornography and privacy.[97]

A report published by UNESCO identifies the following standards regarding intermediary liability:[98]

- Limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression.
- Laws, policies, and regulations requiring intermediaries to impose content restrictions, blocking, and filtering in many jurisdictions are not compatible with international human rights standards for freedom of expression.
- Laws, policies, and practices related to government surveillance and data collection from intermediaries, when insufficiently compatible with human rights norms, impede intermediaries' ability to adequately protect users' privacy.
- Whereas due process generally requires that legal enforcement and decision-making be transparent and publicly accessible, governments are frequently opaque about requests to companies to restrict content, the handover of user data, and other surveillance measures.

There is general agreement that insulating intermediaries from liability for content generated by others protects the right to freedom of expression online. Such insulation can be achieved either through a system of absolute immunity from liability, or a regime that only fixes intermediaries with liability following their refusal to obey an order from a court or other competent body to remove the impugned content.

As to the latter, the 2011 Joint Declaration provides that intermediaries should only be liable for third party content when they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it.[99]

The ECtHR has considered intermediary liability in several cases:

- In 2013, in the case of *Delfi AS v Estonia*, the ECtHR considered the liability of an internet news portal for offensive comments that were posted by readers below one of its online news

[96] Alex Comninos, 'The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain' (2012) at p 6 (accessible at: https://www.apc.org/sites/default/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL_0.pdf).

[97] *Id.*

[98] Rebecca MacKinnon et al, 'Fostering freedom online: The role of internet intermediaries' (2014) at pp 179-180 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000231162_eng).

[99] 2011 Joint Declaration above n 12 at paras 2(a)-(b).

articles.[100] The portal complained that being held liable where the comments of its readers breached the right to freedom of expression. The ECtHR dismissed the case, holding that the finding of liability by the domestic courts was a justified and proportionate restriction of freedom of expression because the comments were highly offensive; the portal failed to prevent them from becoming public, profited from their existence, and allowed their authors to remain anonymous. It further noted that the fine imposed by the Estonian courts was not excessive.

- In 2016, in the case of *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, the ECtHR considered the liability of a self-regulatory body of internet content providers and an internet news portal for vulgar and offensive online comments posted on their websites.[101] The ECtHR reiterated that, although not publishers of comments in the traditional sense, internet news portals still had to assume duties and responsibilities. The ECtHR found that, although offensive and vulgar, the comment was not unlawful speech, and upheld the claim of a violation of the right to freedom of expression.
- In 2017, in the case of *Tamiz v United Kingdom*, the ECtHR had cause to consider the ambit of intermediary liability.[102] The applicant, a former politician in the United Kingdom, had claimed before the domestic courts that a number of third-party comments posted by anonymous users on Google's Blogger.com were defamatory. Before the ECtHR, the applicant argued that his right to respect for his private life had been violated because the domestic courts had refused to grant him a remedy against the intermediary. His claim was ultimately dismissed by the ECtHR on the basis that the resulting damage to his reputation would have been trivial. The ECtHR highlighted the important role that ISPs perform in facilitating access to information and debate on a wide range of political, social and cultural rights, and seemed to endorse the line of argument that ISPs should not be obliged to monitor content or proactively investigate potential defamatory activity on their sites.

---

[100] Application No. 64569/09, 10 October 2013 (accessible at: httsp://hudoc.echr.coe.int/eng?i=001-155105).

[101] Application No 22947/13, 2 February 2016 (accessible at: https://hudoc.echr.coe.int/eng?i=001-160314).

[102] *Tamiz v United Kingdom*, Application No. 3877/14, 19 September 2017 (accessible at: https://hudoc.echr.coe.int/eng?i=001-178106). Media Defence, together with a coalition of organisations, made submissions to the ECtHR on proposed principles for intermediary based on best practices in national legislation, the views of the Committee of Ministers of the Council of Europe (CoE) and special mandate holders.

In the above case before the ECtHR, Media Defence, together with a coalition of other organisations, proposed the following principles:

- Intermediaries should not be the arbiters of the lawfulness of content posted, stored or transferred by the users of their services.
- Assuming that they have not contributed to or manipulated content, intermediaries should not be liable for content posted, stored or transferred using their services unless and until they have failed to comply with an order of a court or other competent body to remove or block specific content.
- Notwithstanding the above, intermediaries should in no circumstances be liable for content unless it has been brought to their attention in such a way that the intermediary can be deemed to have actual knowledge of the illegality of that content.
- A requirement to monitor content on an ongoing basis is incompatible with the right to freedom of expression contained in article 10 of the European Convention on Human Rights.

The submissions are accessible here: https://www.mediadefence.org/sites/default/files/blog/files/20160407%20Tamiz%20v%20UK%20Intervention%20Filing.pdf.

Other courts have taken more definitive positions in respect of intermediary liability. For example, the Supreme Court of India has interpreted domestic law to only provide for intermediary liability where an intermediary has received actual knowledge from a court order, or where an intermediary has been notified by the government that one of the unlawful acts prescribed under the law are going to be committed and the intermediary has subsequently failed to remove or disable access to such information.[103] Furthermore, the Supreme Court of Argentina has held that search engines are under no duty to monitor the legality of third-party content to which they link, noting that only in exceptional cases involving "gross and manifest harm" could intermediaries be required to disable access.[104]

In light of the vital role played by intermediaries in promoting and protecting the right to freedom of expression online, it is imperative that they be safeguarded against unwarranted interference — by state and private actors — that could have a deleterious effect on the right. For example, as an individual's ability and freedom to exercise their right to freedom of expression online is dependent on the passive nature of online intermediaries, any legal regime that causes an intermediary to apply undue restraint or self-censorship toward content communicated through their services will ultimately have an adverse effect on the right to freedom of expression online. The UNSR has noted that intermediaries can serve as an important bulwark against government and private overreach, as they are usually, for instance, best-placed to push back on a shutdown.[105] However, this can only truly be realised in circumstances where intermediaries are able to do so without fear of sanction or penalties.

CONCLUSION

While the right of access to the internet is still arguably in the developmental stages, it is an indispensable enabler of the right to freedom of expression and, as with all human rights, can only be justifiably limited if a three-part test is met. Additionally, restrictions on access to the internet may unduly infringe on freedom of expression and associated rights. In a rapidly developing digital world, the internet is increasingly becoming a contested space, used both by those seeking to defend fundamental rights and those seeking to limit them. The proper understating of concepts such as internet shutdowns, the blocking and filtering of content, net neutrality and intermediary liability are increasingly necessary to fully protect and promote the right to freedom of expression online.

[103] *Shreya Singhal v Union of India*, Application No. 167/2012 at paras 112-118 (accessible at: https://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/).

[104] *María Belén Rodriguez v Google*, Fallo R.522.XLIX (accessible at: http://www.stf.jus.br/repositorio/cms/portalStfInternacional/newsletterPortalInternacionalJurisprudencia/anexo/Fallo_R.522.XLIX__Corte_Suprema_da_Argentina__28_oct._2014.pdf). **Error! Hyperlink reference not valid.**The decision has been described in the 2016 Report of the UNSR on Freedom of Expression at para 52.

[105] 2017 Report of the UNSR on Freedom of Expression, above n 30 at para 50.

MODULE 4: DATA PRIVACY AND DATA PROTECTION

- **The right to privacy is gaining prominence with increasing data flows and the concomitant need for the protection of personal information.**
- **Although South and Southeast Asia lacks a dedicated regional convention on data protection, and there is no such convention for Asia overall, Convention 108 of the Council of Europe is open for accession by non-European states.**
- **States should ensure that their domestic legislation sets out standards for the lawful processing of personal information and that they maintain this legislation in line with data protection developments.**
- **Linked to data protection are the privacy-related concepts of the 'right to be forgotten', encryption and limits on government surveillance.**
- **Notably, the disclosure of journalistic sources as a result of state surveillance has a negative impact on freedom of expression and journalistic freedom.**

INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information or data has garnered significant attention since the dawn of the information age. While the internet and online information-sharing and data collection increase at an exponential rate, legislative developments have failed to keep pace and adequately protect personal information. However, some states have begun to adopt data protection-related instruments and regulations in an attempt to protect the privacy rights of their citizens.

This module focuses on data protection in Asia and the related concepts of the 'right to be forgotten', encryption and surveillance.

THE RIGHT TO PRIVACY

There is increasing recognition that the right to privacy plays a vital role in and of itself and in facilitating the right to freedom of expression. For instance, protection of the right to privacy allows individuals to share views anonymously in circumstances where they may fear being censured for those views, it allows whistle-blowers to make protected disclosures, and it enables members of the media and activists to communicate securely beyond the reach of government surveillance.

The right to privacy is guaranteed in article 12 of the Universal Declaration of Human Rights (UDHR). The right to privacy is also guaranteed in article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides:

> "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> (2) Everyone has the right to the protection of the law against such interference or attacks."

In 2012, the Association of Southeast Asian Nations (ASEAN) member states issued a non-binding declaration reaffirming their commitment to respecting and promoting human rights. Article 21 of the ASEAN Human Rights Declaration closely mirrors the privacy protection in the UDHR, providing:

> Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks.

Interestingly, in 2017, the Supreme Court of India declared that the right to privacy is protected as an intrinsic part of the right to life and personal liberty, and as part of the fundamental freedoms guaranteed by Part III of the Constitution of India.[106] As such, although the Constitution of India does not expressly contain a right to privacy, the right can nevertheless be derived from other rights and freedoms that are constitutionally guaranteed.

As with the right to freedom of expression, a restriction on the right to privacy must comply with the three-part test for such restrictions. As noted by the Supreme Court of India in the 2017 judgment:

> Right to privacy cannot be impinged without a just, fair and reasonable law. It has to fulfil the test of proportionality i.e. (i) existence of a law (ii) must serve a legitimate State aim and (iii) proportionate.[107]

As set out below, we consider specific aspects of the right to privacy and the impact that the internet has had on the enjoyment of this right.

DATA PROTECTION

Data protection laws are aimed at protecting and safeguarding the processing of personal information or personal data, which is defined in the EU's General Data Protection

[106] *Justice K.S. Puttaswamy and Another v Union of India and Others*, Petition No. 494/2012, 24 August 2017 (accessible at: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf).

[107] *Id.* at para 232(vi).

regulation as "any information relating to an identified or identifiable natural person ('data subject')".[108] An "identifiable natural person" is in turn defined as:

> … one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data protection is one of the primary measures through which the right to privacy is given effect. In addition to giving effect to the right to privacy, data protection legislation also has a key role to play in facilitating trade amongst states, as many data protection laws, in particular those adopted within the European Union, restrict cross-border data transfers in circumstances where one state does not provide an adequate level of data protection.

In recent years, increasing attention to the issue of data protection has led to a number of Asian states enacting new privacy laws.[109] Since the onset of the COVID-19 pandemic, the greater reliance on digital technologies for remote working and contact tracing has raised novel challenges with respect to privacy and data protection, adding further momentum and urgency to the need to strengthen data protection laws. Nonetheless, many states continue to protect individuals' privacy only inadequately, especially from state surveillance activities.[110]

In relation to data protection, General Comment No. 16 on article 17 of the ICCPR (General Comment No. 16) provides as follows:[111]

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public

[108] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC at Article 4(1) (accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679).

[109] 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).

[110] 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).

[111] General Comment No. 16 at para. 10.

authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."

Most comprehensive data protection laws typically make provision for the following principles:[112]

- Personal information must be processed fairly and lawfully, and must not be processed unless the stipulated conditions are met.
- Personal information must be obtained for a specified purpose (or purposes) and must not be further processed in any manner incompatible with that purpose.
- Personal data must be adequate, relevant and not excessive in relation to the purpose (or purposes) for which it is processed.
- Personal information must be accurate and, where necessary, kept up to date.
- Personal information must not be kept for longer than is necessary for the purpose of collection.
- Personal information must be processed in accordance with the rights of data subjects provided for under the data protection law, including the right to access, review and where necessary correct the data.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to another country that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108')[113] opened for signature on 28 January 1981 and was the first binding international instrument protecting against abuses stemming from the collection and processing of personal data. The purpose of Convention 108 is to "protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy".[114] Convention 108 provides for the free flow of personal data between states parties to the Convention.

Convention 108 is open for accession by non-members of the Council of Europe. Although a number of non-European member states have acceded to it, no South or Southeast Asian states have yet done so.

[112] Information Commissioner's Office, 'Data protection principles' (accessible at: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/).

[113] Accessible at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[114] Article 1 of Convention 108.

In addition to giving effect to the right to privacy, data protection laws also typically facilitate a right of access to personal information. In this regard, most data protection laws provide for data subjects to request, and be given access to, the information being held about them by a controller. This mechanism can enable data subjects to ascertain whether their personal information is being processed in accordance with the applicable data protection laws, including whether the information held is correct, and whether their rights are indeed being upheld.

'THE RIGHT TO BE FORGOTTEN'

The so-called 'right to be forgotten' — which is perhaps better described as 'the right to erasure' or 'the right to be de-listed' — entails a right to request commercial search engines, such as Google, to remove links to private information when asked. The right to be forgotten progresses from the idea that the right to private life includes a right for past information about oneself, where there is no public interest in accessing, not to be profiled prominently on search results, even though the information will normally remain available on the websites where it is being held.

The leading case on this was decided in 2014, when the Court of Justice of the European Union (CJEU) handed down its ruling in the case of *Google Spain v Gonzalez*.[115] Mr Gonzalez, a Spanish national, lodged a complaint in 2010 with the Spanish information regulator. The cause of Mr Gonzalez's complaint was that, when an internet user entered his name into Google's search engine, the user would obtain links to pages of a Spanish newspaper from 1998 referring to attachment proceedings against him for the recovery of certain debts. Mr Gonzalez requested that the personal data relating to him be removed or concealed because the proceedings against him had been fully resolved and the reference to him was therefore now prejudicial.

The CJEU upheld the claim, relying on the EU data protection law in effect at the time. The CJEU noted that the very display of personal information on a search results page constitutes processing of such information,[116] and there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[117] Further, it was noted that the processing of personal information carried out by a search engine could significantly affect the fundamental rights to privacy and to the protection of personal data when a search is carried out using a person's name, as it enables any internet user to obtain a structured overview of information relating to that individual and establish a profile of the person.[118] According to the CJEU, the effect of the interference "is heightened taking into

[115] *Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another*, Case No. C-131/12, 13 May 2014 (accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131).

[116] *Id* at para 57.

[117] *Id* at para 58.

[118] *Id* at para 80.

account the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous."[119]

With regard to de-listing, the CJEU held that the removal of links from the list of results would also negatively impact the potentially legitimate interests of internet users to access that information, part of their right to freedom of expression.[120] This would require a fair balance to be struck between that interest and those of the data subject, taking into account the nature of the information, its sensitivity for the data subject's private life, and the interest of the public in accessing the information, which would vary according to the role played by the data subject in public life.[121]

The CJEU went on to hold that a data subject is permitted to request that information about him or her no longer be included in a list of search results where, having regard to all the circumstances, the information appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to purposes of the processing carried out by the operator of the search engine, taking into account the public interest in accessing it.[122] In such circumstances, the information should be delinked from search engine results.[123]

The right to be forgotten has also been recognised in domestic contexts. For instance, Italy's Supreme Court of Cassation has held that the public interest in an article diminished after two and a half years, and that sensitive private information should not be available to the public indefinitely.[124] The case was brought before the European Court of Human Rights, which found the restriction on freedom of expression to be justifiable after declining to interfere with Italy's Supreme Court of Cassation's balancing of this right with the right to respect for one's private life.[125] The Belgian Court of Cassation has also recognised the right to be forgotten.[126]

---

[119] *Id.*

[120] *Id* at para 81.

[121] *Id.*

[122] *Id.* at para 94.

[123] *Id.* at para 94.

[124] *Plaintiff X v PrimaDaNoi*, Case No. 13161, 22 November 2015 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/plaintiff-x-v-primadanoi/).

[125] Application no. 77419/16 (2022) at 69-70 (accessible at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Biancardi%20v.%20Italy%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-213827%22]}

[126] *P.H. v O.G.*, Case No. 15/0052/F, 29 April 2016 (accessible at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/06/download_blob.pdf). For a discussion of the case, see Hunton & Williams, 'Belgian Court of Cassation rules on right to be forgotten', 1 June 2016 (accessible at: https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/).

For more on the right to be forgotten, see *NT1 & NT2 v Google LLC* in the UK (2018) (accessible at: https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-nt2-v-google-press-summary-180413.pdf).

There are, however, limits to the ambit of the right to be forgotten. In 2017, the CJEU was seized with a request for a preliminary ruling in the case of *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*.[127] Mr Manni, relying on the *Gonzalez* decision, sought an order requiring the Chamber of Commerce to erase, anonymise or block any data in the register of companies linking him to the liquidation of his company. The CJEU declined to uphold Mr Manni's request and held that in light of the range of possible legitimate uses of data in companies registers and the different limitation periods applicable to such records, it was impossible to identify a suitable maximum retention period. Accordingly, the CJEU declined to find that there is a general right to be forgotten from public company registers.

Furthermore, other jurisdictions have refused to uphold a right to be forgotten vis-à-vis search engines. In Brazil, for example, it was held that search engines cannot be compelled to remove search results relating to a specific term or expression;[128] similarly, the Supreme Court of Japan declined to enforce the right to be forgotten against Google, finding that deletion "can be allowed only when the value of privacy protection significantly outweighs that of information disclosure".[129]

In India, the law on the right to be forgotten remains unsettled. Certain judicial decisions have given effect to the right to be forgotten as a corollary of the right to privacy. For example, the Orissa High Court of the state of Odisha[130] and the High Court of Kerala[131] both found that survivors of sexual violence have a right to have certain online information removed (in the former case non-consensual images in the form of uploaded videos and photos and in the latter case identifying information in a judgment). In 2021, the High Court of Delhi issued an order to block search results for a judgment posted online relating a charge of which the petitioner had been acquitted.[132] In contrast, in 2017, the High Court of Gujarat rejected a similar petition for the removal of a judgment.[133] To date, India continues to lack a comprehensive legislative framework governing the right to be forgotten,

---

[127] Case No. C-385-15, 9 March 2017 (accessible at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=446798).

[128] *Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others*, 2011/0307909-6, 26 June 2012 (accessible at: https://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf).

[129] The Japan Times, 'Top court rejects 'right to be forgotten' demand', 1 February 2017 (accessible at: https://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#.WqZQXehubIV).

[130] *Subhranshu Rout v. State of Odisha*, High Court of Orissa, BLAPL No.4592 of 2020 (2020), (accessible at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/01/Official-Judgment.pdf).

[131] The Case of the Rape Survivor's Right to Be Forgotten, Kerala High Court in the Civil Writ Petition No. 9478 of 2016 (2017), as summarised by Columbia Freedom of Expression due to absence of availability of original decision (accessible at: https://globalfreedomofexpression.columbia.edu/cases/the-case-of-the-rape-survivors-right-to-be-forgotten-india/).

[132] *Jorawar Singh Mundy v. Union of India and Others*, (2021) W.P. (C) 3918/ 2020 (2021) (accessible at: https://www.livelaw.in/pdf_upload/161863647742920 21-393948.pdf).

[133] *Dharamraj Bhanushankar Dave v. State of Gujarat*, Special Civil Application No. 1854 of 2015 (2017), (accessible at: https://indiankanoon.org/doc/156866860/).

although proposed legislation in the form of the *Personal Data Protection Bill*, first introduced in 2019, includes provisions codifying this right.[134]

According to Article 19's Global Principles of Freedom of Expression and Privacy (Global Principles),[135] the right — to the extent that it is recognised in a particular jurisdiction — should be limited to the "right of individuals to request search engines to delist inaccurate or out-of-date search results produced on the basis of a search for their name."[136] It states further that de-listing requests should be "subject to ultimate adjudication by a court or independent adjudicatory body with relevant expertise in freedom of expression and data protection law."[137]

ENCRYPTION AND ANONYMITY ON THE INTERNET

Encryption refers to an automated process of converting messages, information or data into a form unreadable by anyone except the intended recipient, and in doing so protecting the confidentiality and integrity of content against third party access or manipulation.[138] With a "public key encryption" — the dominant form of end-to-end encryption for data in transit — the sender uses the recipient's public key to encrypt the information, and the recipient uses her or his own private key to decrypt it.[139] It is also possible to encrypt data that is stored on one's device, such as a laptop or smartphone.[140]

Anonymity can be defined either as acting or communicating without using or presenting one's name or identity, or as acting or communicating in a way that makes it impossible to determine one's name or identity, or using an invented or assumed name that is not associated with one's legal or customary identity.[141] Anonymity may be distinguished from

---

[134] Ipleaders, Rachit Garg, 'Personal Data Protection Bill, 2019 and the right to be forgotten' (2022), (accessible at: https://blog.ipleaders.in/personal-data-protection-bill-2019-and-the-right-to-be-forgotten/#:~:text=The%20right%20to%20be%20forgotten%2C%20is%20the%20right%20of%20the,it%20is%20no%20longer%20needed).

[135] The Global Principles (accessible at: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf) were developed by civil society, led by ARTICLE19, in cooperation with high-level experts from around the world.

[136] Principle 18(1) of the Global Principles.

[137] *Id* at principle 18(2).

[138] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, 22 May 2015 (UNSR Report on Anonymity and Encryption) at para 7 (accessible at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx). For further discussion and resources, see UCI Law International Justice Clinic, 'Selected references: Unofficial companion report to Report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and freedom of expression' (accessible at: http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf).

[139] *Id.*

[140] *Id.*

[141] Electronic Frontier Foundation, *Anonymity and encryption*, 10 February 2015 at p 3 (accessible at: https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf).

pseudo-anonymity: the former refers to taking no name at all, whilst the latter refers to taking an assumed name.[142] Here again, it is common to reveal the identity to chosen users.

Encryption and anonymity are necessary tools for the full enjoyment of digital rights and enjoy protection by virtue of the critical role that they play in securing the rights to freedom of expression and privacy. As described by the United Nations Special Rapporteur (UNSR) on freedom of expression:[143]

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression."

Encryption and anonymity are especially useful for the development and sharing of opinions online, particularly in circumstances where people may be concerned that their communications may be subject to interference or attack by state or non-state actors. These are therefore specific technologies through which individuals may exercise their rights. Accordingly, any restrictions on encryption and anonymity must meet the three-part test.

According to the UNSR on freedom of expression, while encryption and anonymity may frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public justifications to support restrictions on their use or to identify situations where such restrictions are necessary to achieve a legitimate goal.[144] Outright prohibitions on the individual use of encryption technology disproportionately restrict the right to freedom of expression as they deprive all online users in a particular jurisdiction of the right to use these tools to carve out a space for opinion and expression, regardless of whether or not they are being used for unlawful ends.[145] Likewise, state regulation of encryption may be tantamount to a ban, for example through requiring licences to use encryption, setting weak technical standards for encryption or controlling the import and export of encryption tools.[146]

---

[142] *Id.*

[143] UNSR Report on Anonymity and Encryption above n 33 at para 12.

[144] *Id.* at para 36.

[145] *Id.* at para 40.

[146] *Id.* at para 41.

The UNSR on freedom of expression has called on states to promote strong encryption and anonymity, and noted that decryption orders should only be permissible when they result from transparent and publicly-accessible laws applied solely on a targeted, case-by-case basis to individuals (not to a group of people), and subject to a judicial warrant and the protection of due process rights of individuals.[147]

GOVERNMENT-LED DIGITAL SURVEILLANCE

Communications surveillance encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.[148] This relates to both the content of communications and metadata about them, such as their location and connection points. In respect of the latter, it has been noted that the aggregation of metadata may give deep insight into an individual's behaviour, social relationships, private preferences and identity. Taken as a whole, it may allow very precise conclusions to be drawn concerning the private life of a person.

UN Human Rights Committee General Comment No. 16 provides: "Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto".[149] Surveillance — both bulk (or mass) collection of data[150] or targeted collection of data — interferes directly with the privacy and security necessary for freedom of opinion and expression, and must be considered against the three-part test to assess its legitimacy.[151] In the digital age, Internet and Communications Technologies (ICTs) have enhanced the capacity of governments, corporations and individuals to conduct surveillance, interception and data collection, such that the ability to conduct such surveillance is no longer limited by scale or duration.[152]

---

[147] *Id.* at paras 59-60.

[148] Necessary and proportionate: International principles on the application of human rights to communications surveillance, 2014 (Necessary and Proportionate Principles) at p 4 (accessible at: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf).

[149] General Comment No. 16 at para 8.

[150] Revelations by whistle-blowers, such as Edward Snowden, have revealed that the National Security Agency in the USA and the General Communications Headquarters in the United Kingdom had developed technologies allowing access to much global internet traffic, including records in the United States, individuals' electronic address books and huge volumes of other digital communications' metadata. These technologies are deployed through a transnational network comprising strategic intelligence relationships between governments and other role-players. This is referred to as bulk or mass surveillance. For more on the privacy concerns raised by the Snowden revelations, see Report of the Special Rapporteur on the right to privacy, UN Doc. A/HRC/34/60 (2017) (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/260/54/PDF/G1726054.pdf?OpenElement).

[151] 2016 Report of the UNSR on Freedom of Expression on Contemporary challenges to freedom of expression, UN Doc. A/71/373 at para 20 (accessible at: https://undocs.org/Home/Mobile?FinalSymbol=A%2F71%2F373&Language=E&DeviceType=Desktop&LangRequested=False).

[152] Report of the Special Rapporteur on the promotion and protection of the right to freedom

A resolution adopted by the UN General Assembly (UNGA) on the right to privacy in the digital age emphasised that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, are highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, especially when undertaken on a mass scale.[153] It noted further that "surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory."[154]

In order to meet the condition of legality, many states have taken steps to reform their surveillance laws to authorise surveillance activities. According to the Necessary and Proportionate Principles (a series of principles on the application of human rights to surveillance elaborated by experts and privacy groups), communications surveillance should be regarded as a highly intrusive act, and in order to meet the threshold of proportionality, the state should be required at a minimum to establish the following before a competent judicial authority prior to conducting any surveillance:[155]

- 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.
- There is a high degree of probability that evidence relevant and material to such a serious crime or specific threat would be obtained by accessing the protected information sought.
- Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option.
- Information accessed will be confined to that which is relevant and material to the serious crime or specific threat.
- Any excess information collected will not be retained, but instead will be promptly destroyed or returned.
- Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
- The surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or other fundamental freedoms.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference on the right to hold opinions without interference and the right

---

of opinion and expression, Frank La Rue, A/HRC/23/40 (2013) (accessible at: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf).

[153] UNGA, 'Resolution on the right to privacy in the digital age', A/C.3/71/L.39/Rev.1, 16 November 2016 (2016 UN Resolution on Privacy) (accessible at: https://daccess-ods.un.org/tmp/3401807.84463882.html).

[154] *Id.*

[155] Above at n 43, p. 8.

to freedom of expression. With particular reference to the right to hold opinions without interference, surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing the information needed to form opinions, particularly where such surveillance leads to repressive outcomes.[156]

The interference with the right to freedom of expression is particularly apparent in the context of journalists and members of the media who may be placed under surveillance as a result of their journalistic activities. As noted by the Secretary-General of the UN, this can have a chilling effect on the enjoyment of media freedom and renders it more difficult to communicate with sources and share and develop ideas.[157] The use of encryption and other similar tools have become essential to the work of journalists to ensure that they are able to conduct their work without interference.

The disclosure of journalistic sources through surveillance can have serious negative consequences for the right to freedom of expression due to confidential sources losing trust that journalists will be able to conceal their identities.[158] This is the same for cases concerning the disclosure of anonymous user data. Once confidentiality is undermined, it cannot be restored. It is, therefore, of utmost importance that measures that undermine confidentiality are not undertaken arbitrarily.

Surveillance activities carried out against journalists risk fundamentally undermining the right of source protection to which journalists are otherwise entitled.[159] The increased use of digital technologies and increasingly sophisticated surveillance tools have raised additional challenges for maintaining the anonymity of sources, including due to the risk of

---

[156] UNSR Report on Anonymity and Encryption, above n 33 at para 21.

[157] Report of the Secretary-General on the UN to the UNGA, 'Report on the safety of journalists and the issue of impunity', A/70/290, 6 August 2015 (2015 Report of the UN Secretary-General) at paras 14-16 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/247/06/PDF/N1524706.pdf?OpenElement).

[158] For more, see *Big Brother Watch v United Kingdom* in the ECtHR (2018) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/).

[159] According to principle 9 of the Global Principles, states should provide for the protection of the confidentiality of sources in their legislation and ensure that:

- Any restriction on the right to protection of sources complies with the three-part test under international human rights law.
- The confidentiality of sources should only be lifted in exceptional circumstances and only by a court order, which complies with the requirements of a legitimate aim, necessity, and proportionality. The same protections should apply to access to journalistic material.
- The right not to disclose the identity of sources and the protection of journalistic material requires that the privacy and security of the communications of anyone engaged in journalistic activity, including access to their communications data and metadata, must be protected. Circumventions, such as secret surveillance or analysis of communications data not authorised by judicial authorities according to clear and narrow legal rules, must not be used to undermine source confidentiality.
- Any court order must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies.

unintended source disclosure as a result of surveillance of communication devices.[160] For example, certain journalist sources in the US have been identified through telephone and email records.[161] (For more on the protection of journalist sources, please see Module 10 of this training course).

CONCLUSION

As more of the world moves online, data protection is becoming increasingly necessary. In South and Southeast Asia, some headway has been made with increasing numbers of states now having privacy laws in place. However, with the rapid growth in data harvesting, legislators are some way behind in fully protecting and promoting privacy and personal data protection. As we move forward, digital rights activists have a significant role to play in ensuring that states keep up-to-date with data protection developments and enact legislative frameworks which fully protect and promote people's rights to privacy.

[160] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/70/361 (2015), para. 23 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/273/11/PDF/N1527311.pdf?OpenElement).
[161] See, for example, *United States of America v. Sterling*, 724 F.3d 482 (2013).

MODULE 5: DEFAMATION

- **Defamation is frequently used to unjustly stifle dissent. However, it can provide a genuine remedy for those whose reputations are harmed by the statements or actions of others.**
- **Criminal defamation is generally considered to be disproportionate under international law. Even civil defamation is often punished too harshly, going beyond just righting the wrong that was committed.**
- **Truth is a core defence against defamation claims.**
- **Some types of speech should not be subject to defamation actions, such as opinions and satire.**
- **The growth of SLAPP[162] suits by corporate actors using defamation laws to silence or intimidate those who criticise them is a concerning contemporary development that needs to be addressed.**

INTRODUCTION

The use of meritless defamation proceedings is a notorious method of stifling freedom of expression and dissent, particularly of journalists. While defamation laws aim to provide individuals with a remedy for public statements that harm their reputation, they inevitably come into conflict with the right to freedom of expression. Correctly balancing the protection of freedom of expression and the public's right to information with protecting individuals' reputations is central to the appropriateness or otherwise of defamation laws and claims.

The impact of the internet, and particularly social media networks, has meant that it is easier than ever to publish content to a wide audience. As a result, defamation proceedings have become a commonly used instrument wielded against the authors of statements published online, whether justifiably so or not, while also contributing to a significant increase in defamatory statements.

The ability to freely post information on social media and the internet without the same degree of thought and review as traditional media, combined with a lack of awareness about defamation laws and the fact that many countries have adopted vague legal rules governing online defamation has led to an increase in online defamation cases and some ambiguity in how defamation applies online.[163]

[162] Strategic Lawsuits Against Public Participation.
[163] On the use of overbroad defamation provisions to target online speech, see International Commission of Jurists, *Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia* (2019) (accessible at: https://www.icj.org/wp-content/uploads/2019/12/Southeast-Asia-Dictating-the-Internet-Publications-Reports-Thematic-reports-2019-ENG.pdf).

Dealing with online defamation cases is particularly challenging for many reasons. The online environment can make it more difficult to identify or trace authors, and victims may want to consider whether to pursue the author or the system operator, since some legal systems consider anyone who participates in distributing defamatory statements to be equally liable. In addition, deciding the jurisdiction of the court to hear the matter can be difficult as messages posted online are available all over the world, and the parties to a dispute may come from and be located in different jurisdictions.

This module provides an overview of defamation laws in the context of South and Southeast Asia and how courts have attempted to strike a balance between various rights in recent jurisprudence, with a particular focus on online defamation cases.

WHAT IS DEFAMATION?

Defamation is a false statement of fact that is harmful to someone's reputation.[164] The law of defamation dates back to the Roman Empire, but while the penalties and costs attached to defamation today are often not as serious as they once were, they can still have a notorious "chilling effect," with prison sentences or massive compensation awards posing a particularly serious risk to freedom of expression, journalistic freedom, and dissent in many countries.

The foundation for defamation in international law is article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides for protection against unlawful attacks on a person's honour and reputation. Article 19(3) of the ICCPR also makes reference to the rights and reputation of others as a legitimate ground for restricting freedom of expression.[165] Reputation is therefore the underlying basis in any claim of defamation.[166]

There are many examples where defamation suits serve an important purpose in providing a remedy for victims of slanderous and harmful attacks on their reputations. However, defamation is also frequently misused, particularly by states and officials but also by non-state actors to stifle free speech, including through SLAPP suits.

CRIMINAL DEFAMATION

Historically, defamation was usually a criminal offence. While many countries still have the offence of criminal defamation on their statute books, it is widely considered to be problematical as a restriction on freedom of expression, including by the United Nations (UN), which has urged states to reconsider such laws. For instance, the UN Human Rights Committee (UNHRCtte) General Comment No. 34 provides that: "States Parties should consider the decriminalisation of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty".[167]

---

[164] Article 19, Defamation ABC at p. 1 (accessible at https://www.article19.org/data/files/pdfs/tools/defamation-abc.pdf). Under some legal systems, especially common law jurisdictions such as India and Pakistan, libel is the term used for a written defamatory statement, while slander refers to spoken defamation.
[165] ICCPR: International Covenant on Civil and Political Rights (1976) (accessible at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx).
[166] For a fuller discussion on the law on defamation, see Article 19, Defamation ABC, note 3.
[167] UN Human Rights Committee, 'General Comment No. 34 at article 47 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).

The use of criminal sanctions in defamation proceedings in Southeast Asia came under scrutiny by the UN Human Rights Committee in the case of *Alexander Adonis v. The Philippines*,[168] in which the Committee considered an individual complaint by a radio broadcaster who had been convicted of criminal defamation. The author of the complaint alleged that the conviction was inconsistent with article 19 of the ICCPR because less restrictive measures could have been employed instead, the unavailability of a defence of truth except in narrow circumstances, the unavailability of a defence of public interest and the presumption of malice that had the effect of placing the burden of proof on the defendant.[169] The Committee found that the conviction in these circumstances was an unjustifiable restriction on freedom of expression which was incompatible with article 19(3) of the ICCPR.[170]

Despite the evolution of international standards towards considering criminal defamation to be a disproportionate restriction on freedom of expression, many countries retain criminal defamation laws. There have, however, been certain positive developments over the years. Notably, in 2002, Sri Lanka amended its Criminal Code to remove the offence of criminal defamation.[171]

Protections against criminal defamation laws

When a criminal defamation law remains on the statue book, there are a number of strict protections that should at a minimum apply to prevent defamation from being used to stifle freedom of expression:[172]

- The criminal standard of proof — beyond a reasonable doubt — should be fully satisfied.[173]
- Convictions for criminal defamation should only be secured when the allegedly defamatory statements are false, and when the mental element of the crime is satisfied, i.e. when they are made with the knowledge that the statements were false or with reckless disregard as to whether they were true or false.
- Penalties should not include imprisonment or suspensions of the right to freedom of expression or the right to practice journalism.[174]

[168] CCPR/C/103/D/1815/2008/Rev.1 (2008) (accessible at https://juris.ohchr.org/Search/Details/1613).
[169] *Id.* at para 7.7.
[170] *Id.* at para 7.10.
[171] Zee News, 'Sri Lanka abolishes criminal defamation' (2002) (accessible at https://zeenews.india.com/news/south-asia/sri-lanka-abolishes-criminal-defamation_45922.html).
[172] Toby Mendel, *Defining Defamation Principles on Freedom of Expression and Protection of Reputation* (Article 19, 2000) at Principle 4 (accessible at: https://www.article19.org/wp-content/uploads/2018/02/defining-defamation.pdf).
[173] Inter-American Court of Human Rights, *Kimel v. Argentina*, (2008) (accessible at: https://www.corteidh.or.cr/docs/casos/articulos/seriec_177_ing.pdf).
[174] See for example: African Court of Human and Peoples' Rights, *Konaté v. Burkina Faso*, Application No. 004/2013 (2014) (accessible at: http://www.ijrcenter.org/wp-content/uploads/2015/02/Konate-Decision-English.pdf).

- As a less restrictive means, states should not resort to criminal law when a civil law alternative is readily available.[175]

CIVIL DEFAMATION

Despite widespread agreement that criminal punishment for defamation is no longer acceptable, there is nevertheless a need for some sort of remedy for those whose reputations have been unfairly harmed.

Therefore, almost all countries have domestic laws providing protection against defamation, but these laws vary by jurisdiction. In some countries, defamation laws are overly restrictive vis-à-vis freedom of speech, for example by limiting criticism of leaders or by providing for disproportionately harsh sanctions. Another challenge to freedom of expression is that some judges and juries elect to award disproportionately large damages in civil defamation matters.

If a person is able to prove a civil claim for defamation, and the person responsible for the statement or publication is not able to raise a successful defence, the person who has suffered reputational harm is typically entitled to monetary compensation in the form of reasonably quantified civil damages. While civil defamation claims may serve the intended purposes of restoring reputation or honour, they can be abused and cause a "chilling effect" on the full enjoyment and exercise of freedom of expression.

CAN A TRUE STATEMENT BE DEFAMATORY?

In most jurisdictions, consistent with international law, truth is an absolute defence to a defamation claim. However, in some jurisdictions, truth alone is not sufficient: it is further required that the public interest in the publication be established as well.

Courts in some jurisdictions have also held that even false statements may be protected against a defamation claim. In *Rajagopal & Anor v. State of Tamil Nadu*,[176] decided by the Indian Supreme Court, a key issue was whether public officials could prevent the publication of a biography that they claimed defamed them. The Court discussed a number of leading authorities and concluded that even untrue statements about officials would not sustain a defamation claim unless they were published recklessly:

> In the case of public officials ... the remedy of action for damages is simply not available with respect to their acts and conduct relevant to the discharge of their official duties. This is so even where the publication is based upon facts and statements which are not true, unless the official established that the publication was made (by the defendant) with reckless disregard for truth.[177]

---

[175] See for example: European Court of Human Rights, *Amorim Giestas and Jesus Costa Bordalo v. Portugal*, Application No. 37840/10 (2014), para. 36 (accessible at: https://hudoc.echr.coe.int/eng?i=001-142084 in French).
[176] *Rajagopal & Anor v. State of Tamil Nadu,* [1994] 6 SCC 632 (SC) (accessible at: https://indiankanoon.org/doc/501107/).
[177] *Id.*, para 26.

In their 2000 Joint Declaration, which focused, among other things, on defamation, the special international mandates on freedom of expression stated:

> At a minimum, defamation laws should comply with the following standards:
> …
> ▪ it should be a defence, in relation to a statement on a matter of public concern, to show that publication was reasonable in all the circumstances.[178]

Similarly, General Comment No. 34 states that "a public interest in the subject matter of the criticism should be recognised as a defence"[179] against defamation.

THE RIGHT TO PROTECTION AGAINST ATTACKS ON REPUTATION

The right to protection against attacks on reputation is firmly established in international law. Article 12 of the Universal Declaration of Human Rights provides that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[180] This is echoed in identical words in article 17 of the ICCPR.

Therefore, as indicated above, a balance often needs to be found between protecting individuals from false and harmful attacks on their reputation on the one hand and freedom of expression and the public's right to information on the other.

WHAT IS THE RIGHT WAY TO DEAL WITH ONLINE DEFAMATION?

When a person is found to have been defamed, they are entitled to a remedy. However, in practice, the rules on defamation are often punitive and disproportionate. We have already seen that sentences of imprisonment for criminal defamation are disproportionate due to their impact on freedom of expression.[181] Likewise, fines or damage awards should not be excessively punitive and should instead be aimed at remedying the harm done.

Whenever possible, redress in defamation cases should be non-pecuniary (non-financial) and aimed directly at remedying the wrong caused by the defamatory statement, such as through publishing an apology or correction.

Monetary awards — the payment of damages — should only be considered when other less intrusive means are insufficient to redress the harm caused. Compensation for harm caused (pecuniary damages) should be based on evidence quantifying the harm and the demonstration of a causal relationship with the alleged defamatory statement.

---

[178] Joint Declaration on Current Challenges to Media Freedom (2000) (accessible at: https://www.osce.org/files/f/documents/c/b/40190.pdf).
[179] General Comment 34 above n 6 at p 12.
[180] UN General Assembly, 'Universal Declaration of Human Rights, Resolution 217 A (III)' (1948) (accessible at: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf).
[181] General Comment 34 above n 6.

Defamation on new media platforms

The growth of social media in recent years has raised questions about whether existing civil defamation laws and doctrines are adequate. One challenge is the difficulty of adapting remedies to the online era. As detailed in Module 2, once defamatory information is published online, it can be difficult to order it fully removed due to the potential for social media content to 'go viral'.

Another issue that has arisen in various jurisdictions is whether to treat hyperlinks to defamatory content as akin to publication of this content. Clearly a rigid approach that views all hyperlinks as amounting to publication would have a chilling effect on online expression. However, courts have had to grapple with the thornier question of whether such links can ever be treated as publications.

In *Crookes v. Newton,* the Supreme Court of Canada held that the use of basic hyperlinks cannot alone, in the absence of actually repeating specific content, count as publication of defamatory material.[182] However, the majority declined to offer any definitive approach to more complex links (such as those embedded in text or images that automatically display content without leaving the original webpage), noting the "inherent and inexorable fluidity of evolving technologies" that made it "unwise in these reasons to attempt to anticipate, let alone comprehensively address, the legal implications of the varieties of links that are or may become available".[183] A minority opinion did not agree with the majority's approach of not treating any basic hyperlinks as publications and instead preferred a more contextual approach to assessing whether "the text that includes the hyperlink constitutes adoption or endorsement of the specific content it links to"[184] while, in another separate opinion, one justice advocated for an approach based on assessing whether a defendant had, on a balance of probabilities, deliberately made defamatory content readily available.[185]

In *Magyar Jeti Zrt v. Hungary*[186], the European Court of Human Rights established a more contextual approach towards assessing liability for use of hyperlinks to defamatory content, requiring an individual assessment, taking into account the following factors:

(i) did the journalist endorse the impugned content;
(ii) did the journalist repeat the impugned content (without endorsing it);
(iii) did the journalist merely include a hyperlink to the impugned content (without endorsing or repeating it
(iv) did the journalist know or could he or she reasonably have known that the impugned content was defamatory or otherwise unlawful;
(v) did the journalist act in good faith, respect the ethics of journalism and perform the due diligence expected in responsible journalism?[187]

In *Loong v. Hiang*,[188] the High Court of Singapore considered a Facebook post that contained a link to an article that was alleged to contain defamatory material about Singapore's Prime Minister, in particular, reports that investigations were "trying to find the secret deals between the two corrupted Prime Ministers of Singapore and Malaysia."[189] The High Court rejected the 'bright line' approach to basic hyperlinks adopted by the majority of the Supreme Court of Canada, instead opting for a "more holistic assessment", citing Australian and British jurisprudence that the Court noted relied upon the European Court of Human Rights' judgment in *Magyar Jeti Zrt*.[190] In applying the contextual approach, the High Court found that the linked article should be deemed part of

the Facebook post after reasoning that the link contained no other content other than the link to the article and finding that there was no plausible interpretation of the article other than an endorsement of its content.[191]

Although *Loong v. Hiang* is an example of attempts to grapple with how to approach hyperlinks and of the cross-pollination of European Court of Human rights and national constitutional jurisprudence on this matter, the Court's ultimate decision to award damages in a case involving content critical of the Prime Minister raises significant concerns from an international human rights perspective. This case is part of an unfortunate pattern of Singapore's leaders bringing defamation suits against journalists and political opponents,[192] which can have a chilling impact on freedom of expression. The UN Human Rights Committee, the European Court of Human Rights, the Inter-American Court of Human Rights and the African Court on Human and Peoples' Rights have all underscored that political speech directed against government officials deserves a particularly high degree of protection in view of the public interest in open political debate.[193]

TYPES OF POTENTIALLY DEFAMATORY STATEMENTS

Opinions versus statements of fact

We discussed above factual statements that may be defamatory. However, expressions of opinion are differentiated from factual statements. General Comment No. 34 states that defamation laws, particularly penal defamation laws, "should not be applied with regard to those forms of expression that are not, of their nature, subject to verification,"[194] such as opinions and value judgments. It also notes: "All forms of opinion are protected, including opinions of a political, scientific, historic, moral or religious nature."

---

[182] 2011 SCC 47, [2011] 3 SCR 269 (2011) (accessible at: https://www.canlii.org/en/ca/scc/doc/2011/2011scc47/2011scc47.html).
[183] *Id.* at para 43 (opinion of Abella J for the majority, joined by Binnie, LeBel, Charron, Rothstein and Cromwell JJ).
[184] *Id.* at para. 50 (opinion of Fish J, joined by McLachlin C.J.).
[185] *Id.* at para. 93 (opinion of Deschamps J.)
[186] Application No. 11257 (2019) (accessible at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2211257/16%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-187930%22]}).
[187] *Id.* at para 77.
[188] [2021] SGHC 66 (2021), (accessible at: https://www.elitigation.sg/gd/s/2021_SGHC_66).
[189] *Id.* at para 5.
[190] *Id.* at para. 41.
[191] *Id.* at para. 42.
[192] Committee to Protect Journalists, 'New York Times to pay damages to Singapore's leaders' (2010) (accessible at: https://cpj.org/2010/03/new-york-times-to-pay-damages-to-singapores-leader/).
[193] General Comment 34 at para. 38; *Magyar Jeti Zrt v. Hungary*, above at n 44, paras. 81-82; *Ricardo Canese v. Paraguay*, Merits, Reparations and Costs, H.R. (ser. C) No. 111 (2004) at para. 103 (accessible at: https://www.corteidh.or.cr/docs/casos/articulos/seriec_111_ing.pdf; and *Ingabire Victoire Umuhoza v. Rwanda*, Application No. 003/2014 (2017) at para. 142 (accessible at: https://www.african-court.org/en/images/Cases/Judgment/003-2014-Ingabire%20Victoire%20Umuhoza%20V%20Rwanda%20-%20Judgement%2024%20November%202017.pdf).
[194] General Comment 34 at n 6 at p 12.

To determine what counts as an opinion, courts tend to look at whether a reasonable person would understand the statement as asserting a statement of verifiable fact, which is capable of being proven to be true or false. In the context of social media, a reasonable reader tends to be defined as someone who would ordinarily be following and reading the statement. The Singapore High Court has applied a somewhat broader definition of the 'ordinary reasonable person' as someone "assumed to possess general knowledge and experience of worldly affairs".[195]

The context in which the statement was made is critical to determining whether a reasonable person would understand it as an opinion or as a statement of fact. There are, for example, ways in which a statement of opinion may appear to be factual in nature.[196] In 2020, a US District Court dismissed a defamation lawsuit against controversial Fox News talk show host Tucker Carlson, noting that the "'general tenor' of the show should then inform a viewer that [Carlson] is not 'stating actual facts' about the topics he discusses and is instead engaging in 'exaggeration' and 'non-literal commentary.'"[197]

Humour

Similarly, content that a reasonable person would identify as humour or satire, rather than as stating a fact, should also be treated as an opinion. For example, the Malaysian Court of Appeal has stated that:

> No reasonable person will read a cartoon with the same concentration, contemplation and seriousness as one would when reading a work of literature. Cartoons exaggerate, satirize and parody life, including political life. […] The political cartoonist, unlike the serious political pamphleteer, seeks to ridicule persons and institutions with humour to deliver a message. It will be most exceptional if a political cartoon will have the effect of disrupting public order, security or the safety of the nation.[198]

The Supreme Court of India came to a similar conclusion in respect of a film containing a song that was deemed offensive to the Bata India footwear company, concluding:

> [T]he song appears to have been written in the context of the theme of the film and ought not be taken as any kind of aspersion against the persons named in said song.[199]

Statements of others

A point of consideration, particularly for journalists, is the extent to which they are liable for repeating defamatory statements of others since a central part of their work is reporting on the words of others.

---

[195] *Loong v. Hiang*, above at n 27 at para. 26.
[196] Electronic Frontier Foundation, 'Online Defamation Law' (accessible at https://www.eff.org/issues/bloggers/legal/liability/defamation#:~:text=Generally%2C%20defamation%20is%20a%20false,slander%20is%20a%20spoken%20defamation .
[197] US District Court, Southern District of New York, Case No. 1:2019cv11161 - Document 39' (2020) (accessible at: https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2019cv11161/527808/39/).
[198] Malaysian Court of Appeal, *Zulkiflee Bin SM Anwar Ulhaque v. Arikrishna Apparau* (*Zunar Case*), Civil Appeal No. W-01-500-2011 (2014).
[199] *Bata India Limited v. Prakash Jsh Prodcutions And Others*, (Record of Proceedings), SLP (C) No. 32998 (2012) (accessible at: https://www.casemine.com/judgement/in/56e0fa97607dba3896607a0a).

The European Court of Human Rights (ECtHR) has found that a journalist is not automatically liable for quoting opinions of others, and is not required to "systematically and formally" distance themselves from "the content of a statement that might defame or harm a third party,"[200] provided they have not repeated potentially defamatory statements as their own, endorsed, or clearly agreed with them.

Privileged statements

Privileged statements refer to certain statements which receive protection against defamation liability due the public interest in this based on the circumstances in which they were made. Statements from legislature or judicial proceedings are usually considered absolutely privileged, meaning that neither the author of the statement nor a fair media report on it may be held liable for defamation. A number of other statements which involve social or moral responsibilities – such as giving a reference on someone or reporting a crime to the police –also enjoy qualified privilege, which means they are protected unless they were made with malice.

Whose burden of proof?

A general principle of law is that the burden of proof lies with the claimant — the person who brings the suit or makes the "claim". However, with defamation, this principle is generally reversed, and the responsibility lies with the defendant — the person who made the allegedly defamatory statement — to prove that the statement did not damage the claimant's reputation, either because it is true or for one of the other reasons listed above. The United States is a prominent exception to this rule, wherein the burden of proof of falsity of the statement in cases brought by any public figure falls on the claimant.

However, in defamation cases concerning the public interest, international standards have been evolving towards the US approach to the burden of proof, as articulated by the Supreme Court in *New York Times v. Sullivan*.[201] The special international mandates on freedom of expression have called for the burden of proof to be on the plaintiff in such cases. For example, in their 2000 Joint Declaration, they noted that "the plaintiff should bear the burden of proving the falsity of any statements of fact on matters of public concern".[202] The UN Special Rapporteur on Freedom of Expression has also affirmed that "where truth is an issue, the burden of proof lies with the plaintiff".[203] Nevertheless, a clear consensus on this approach has not yet emerged, with the European Court of Human Rights' dismissing arguments to adopt the *Sullivan* approach in their 2002 judgment in *McVicar v. United Kingdom*.[204]

---

[200] European Court of Human Rights, Application No. 1131/05 (2007).
[201] *New York Times Company v. Sullivan*, 376 U.S. 254 (1964) at para. 40.
[202] 2000 Joint Declaration on Current Challenges to Media Freedom (2000) (accessible at: https://www.osce.org/files/f/documents/c/b/40190.pdf).
[203] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mission to Italy from 11 to 18 November 2013, (2014) at para. 23 (accessible at: https://undocs.org/A/HRC/26/30/Add.3).
[204] Application No. 46311/99 (2002) at para. 87 (accessible at: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-60450&filename=001-60450.pdf).

Remedies and penalties

As discussed above, criminal penalties have been the focus of much attention by international bodies. It is notable that no international human rights court has ever upheld a custodial sentence imposed on a journalist. It is important that civil defamation laws contain sufficient checks and balances on the size of damage awards to prevent them from unduly stifling freedom of expression.

TYPES OF CLAIMS

SLAPP suits

Defamation suits are being abused to silence critics and journalists. The term "strategic lawsuits against public participation" (SLAPPs) is being used to describe cases which aim intentionally to bury critics under expensive and baseless legal claims in order to intimidate and silence them. The objective in these cases is not a positive judgment but rather to leverage the threat of financial damage through costly litigation. Defamation allegations are often used as the underlying complaints in SLAPP suits.

In many cases, courts have found against plaintiffs bringing such suits. For example, in the case of *Raub Australian Gold Mining Sdn Bhd v. Hue Shieh Lee*,[205] a mining company brought a complaint for libel and malicious falsehood before the Malaysian courts against the author of two articles. In these articles, the author had alleged the existence of medical complications suffered by residents in the vicinity of the company's mining operations. Although the suit ultimately failed, the mere threat of costly, protracted litigation against well-financed corporations can have a chilling effect on the freedom of expression of activists and journalists.

A limited number of jurisdictions, such as certain provinces in Canada,[206] have adopted anti-SLAPP legislation to protect freedom of expression by allowing baseless defamation and other cases to be dismissed at an early stage of the proceedings and sometimes also to provide for special remedies for defendants to reclaim costs from the claimants. However, there is a need for much more widespread adoption of such anti-SLAPP laws to protect critical speech. A 2020 study from the Business & Human Rights Resource Centre found that in 2019 Southeast Asia was the region with the second highest incidence of recorded SLAPP suits (after Central America) and that the Philippines was the only state in the region with legislation defining SLAPPs, albeit with its application restricted to environmental cases.[207]

[205] Civil Appeal No. 02(f)-125-11/2017(W) (2017) (accessible at: https://elaw.org/system/files/attachments/publicresource/raub_fedcourt_2019.pdf).
[206] Osler, O'Brien and Tsilivis, 'Ontario Court of Appeal clarifies test under "anti-SLAPP" legislation' (2018) (accessible at: https://www.osler.com/en/resources/regulations/2018/ontario-court-of-appeal-clarifies-test-under-anti-slapp-legislation).
[207] Business & Human Rights Resource Centre, 'Strategic Lawsuits against Public Participation: Southeast Asia cases & recommendations for governments, businesses, & civil society' (2020) (accessible at: https://media.business-humanrights.org/media/documents/files/SLAPPs_in_SEA_2020_Final.pdf).

Online harassment as a method of suppressing dissent

Online harassment of journalists using non-legal means is another too-often used method of stifling freedom of expression and dissent. Women journalists have been found to disproportionately be subjected to online harassment.[208] Online harassment can take many forms, including surveillance, posting threatening messages, hacking, doctoring or sharing personal images and other forms of 'doxxing' (i.e. maliciously sharing personal or identifying information).

Anonymous harassing messages can be difficult to trace but, when part of a broader pattern of online harassment, they may be evidence of a state-sponsored campaign to harass dissidents. In Vietnam, for example, Amnesty International reported dozens of incidents of activists receiving threatening online messages.[209] The report noted that the deputy head of the Vietnamese military's political department had in December 2017 introduced a cyberspace military battalion made up of around 10,000 'cyber-troops' tasked with information warfare and correcting what the government deemed "distorted information on the internet".[210]

Insult laws

A number of insult and other related laws are still in place across Asia and continue to pose risks for journalists and others critical of government. Thailand, for example, has particularly draconian *'lèse majesté'* laws, with one individual receiving a 43-year prison sentence for insulting the royal family, a sentence that elicited condemnation by multiple UN special rapporteurs.[211] Likewise, the crime of sedition remains on the statute books in many countries and continues to be used to stifle freedom of expression. Sedition has been defined as the crime of "incitement of resistance to or insurrection against lawful authority."[212]

A more recent development has been the passing of 'false news' laws in various countries. These laws are justified by states as being necessary to protect national security or public order and to deal with the misinformation pandemic that has been unleashed by the growth of the internet and social media. Inasmuch as they generally prohibit the dissemination of false news, these laws represent a breach of the right to freedom of expression.

The UN Human Rights Committee and regional courts, including the Inter-American Court of Human Rights, the African Court on Human and Peoples' Rights and the European Court of Human Rights, have increasingly argued that public officials should enjoy *less* protection from criticism than others.[213] Because of their status, access to the media, and power, public officials can use their

[208] UNESCO, 'Online violence against women journalists: a global snapshot of incidence and impacts' (2020), accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000375136).
[209] Amnesty International, ' "Let Us Breath!" Censorship and Criminalization of Online Expression in Vietnam' (2020) at p. 51, s. 4.3.2. (accessible at: https://www.amnesty.org/en/documents/asa41/3243/2020/en/).
[210] *Id.* at s. 4.3.3, pp. 52-53.
[211] United Nations Office of the High Commissioner for Human Rights, 'Thailand: UN experts alarmed by rise in use of lèse-majesté laws' (2021) (accessible at: https://www.ohchr.org/en/press-releases/2021/02/thailand-un-experts-alarmed-rise-use-lese-majeste-laws?LangID=E&NewsID=26727).
[212] Merriam Webster Dictionary, 'Sedition' (accessible at: https://www.merriam-webster.com/dictionary/sedition).
[213] See sources in note 32.

office to try to curtail freedom of expression and prosecute critics. Additional protections for those who criticise them may therefore be warranted to counter this imbalance of power. In addition, there is a real need for those serving in public office to be open to criticism and public input. As the European Court found:

> "The [politician] inevitably and knowingly lays himself open to close scrutiny of his every word and deed by both journalists and the public at large, and he must display a greater degree of tolerance, especially when he himself makes public statements that are susceptible of criticism."[214]

The Office of the High Commissioner for Human Rights (OHCHR) has also called for the abolition of the offence of 'defamation of the State,'[215] and some jurisdictions have refused to allow public authorities, as such, to sue for defamation.[216] The ECtHR has limited such suits to situations which threaten public order, implying that governments cannot sue in defamation simply to protect their honour.[217]

CONCLUSION

The criminalisation of defamation poses a serious risk to freedom of expression, particularly with the rise of social media platforms online. Defamation proceedings serve a legitimate purpose of protecting individuals' reputations but are also often abused to silence and punish dissent. Despite the recent trend towards the decriminalisation of defamation, there remains a need to decriminalise in more countries, or at least to remove criminal punishments, to address excessive civil defamation awards, to ensure that defamation laws provide appropriate defences to defendants, and to adopt legal protections against SLAPP suits.

---

[214] *Oberschlick v. Austria,* Application No. 20834/92 (1997), para 29 (accessible at: https://hudoc.echr.coe.int/eng?i=001-58044). For more on this topic, see the seminal case establishing the need for public officials to face a higher threshold of criticism, *New York Times v Sullivan* in the United States Supreme Court, 376 US 254 (1964) at paras. 279-80 (accessible at: https://supreme.justia.com/cases/federal/us/376/254/).

[215] OHCHR, Concluding Observations of the Human Rights Committee: Serbia and Montenegro, CCPR/CO/81/SEMO (12/08/2004) at para. 22 (accessible at: https://www.refworld.org/docid/42ce6cfe4.html).

[216] OHCHR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,' E/CN.4/2000/63 (2000) (accessible at: https://www.ohchr.org/en/issues/freedomopinion/pages/annual.aspx).

[217] *Id.*

MODULE 6: HATE SPEECH

- **Certain types of speech, known as hate speech, are prohibited by international law.**
- **It is important to draw a clear distinction between speech that is offensive or even racist, and yet protected under international guarantees of freedom of expression, and speech which constitutes impermissible hate speech that should legitimately be restricted.**
- **Regulating hate speech can be particularly difficult in the online context.**
- **International law requires states to ban hate speech which intentionally incites to violence, hatred or discrimination, but not that actual harm results.**
- **The biggest danger with hate speech is that vagueness in defining its meaning may allow such laws to be used as tools to stifle legitimate criticism or political speech.**
- **Incitement to genocide is often treated as a special case of hate speech, although care is also needed here to ensure that any restrictions are narrow and legitimate.**

INTRODUCTION

Despite the importance of freedom of expression, not all speech is protected under international law, and some limited forms of speech are required to be prohibited by states. Article 20 of the International Covenant on Civil and Political Rights (ICCPR) provides that:

> "(1) Any propaganda for war shall be prohibited by law.
> (2) Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."

In addition, article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination requires that the dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, shall be declared an offence that is punishable by law.

Hate speech provisions under international law distinguish between three categories of speech: that which should be restricted, that which may be restricted; and that which is lawful and subject to protection, according to the severity of the speech in question. Hate speech regulations vary significantly by jurisdiction, particularly in how they define what constitutes hate speech.

There is a need for clear and narrowly circumscribed definitions of what is meant by the term "hate speech", or objective criteria that can be applied. Over-regulation of hate speech can violate the

right to freedom of expression, while under-regulation may lead to intimidation, harassment or violence against minorities and protected groups.

Importantly, hate speech should not be conflated with offensive speech, as the right to freedom of expression includes speech that is robust, critical, or that causes shock or offence.[218] Hate speech is perhaps the topic that creates the most disagreement among defenders of freedom of expression, as defining the line between offensive but protected speech and hate speech can be extremely difficult.

As a general principle, no one should be penalised for statements that are true. Furthermore, the right of journalists to communicate information and ideas to the public should be respected, including when they are reporting on racism and intolerance, and prior censorship should be applied, if at all, only in the most limited circumstances. Finally, any sanctions for hate speech should be in strict conformity with the principle of proportionality.

There are some distinctions between hate speech online and offline that may require consideration,[219] although laws generally do not distinguish between the two:

- Content is more easily posted online without due consideration or thought. Online hate speech cases need to distinguish between poorly considered statements posted hastily online, and an actual threat that is part of an intentional campaign of hatred.
- Once something is online, it can be difficult (or impossible) to get it off entirely. Hate speech posted online can persist in different formats across multiple different platforms, which can make it difficult to address.
- Online content is frequently posted anonymously, which presents an additional challenge to dealing with hate speech online.
- The internet has transnational reach, which raises cross-jurisdictional complications in terms of legal mechanisms for combatting hate speech and even definitions of it.

WAS "HATE SPEECH" INTENDED TO INCITE?

Hate speech that is intended to incite hostility, discrimination or violence is a type of expression that international law mandates must be restricted. Therefore, a key factor when dealing with hate speech cases is the requirement for there to have been an *intention* to incite hatred.

The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,[220] compiled by a meeting of experts coordinated by the United Nations Office of the High Commissioner for Human Rights (OHCHR),

---

[218] Media Defence, 'Training manual on digital rights and freedom of expression online, at p 57 (2020) (accessible at: https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-digital-rights-and-freedom-of-expression-online/).
[219] Media Defence, 'Training manual on digital rights and freedom of expression online, at p 57 (2020) (accessible at: https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-digital-rights-and-freedom-of-expression-online/).
[220] Office of the High Commissioner for Human Rights (OHCHR), 'Freedom of expression vs incitement to hatred: OHCHR and the Rabat Plan of Action', (2012) (accessible at: https://www.ohchr.org/en/issues/freedomopinion/articles19-20/pages/index.aspx).

proposes a six-part threshold test to establish whether expression rises to the threshold of being criminal. One of these is intent: "advocacy" and "incitement" are required, rather than mere distribution or circulation. Article 20 of the ICCPR also requires intent, as signalled by the word 'advocacy'. Negligence and recklessness therefore do not rise to the standard of hate speech.

A prime example of this distinction is the case of *Jersild v Denmark* decided by the European Court of Human Rights (ECtHR). Jersild was a television journalist who made a documentary featuring interviews with members of a racist, neo-Nazi gang. He was prosecuted and convicted for propagating hate speech. However, the ECtHR found that the journalist's intent was to make a serious social inquiry exposing the views of the racist gangs, not to promote their views. There was a clear public interest in the media playing such a role:

> "Taken as a whole, the feature could not objectively have appeared to have as its purpose the propagation of racist views and ideas. On the contrary, it clearly sought - by means of an interview - to expose, analyse and explain this particular group of youths, limited and frustrated by their social situation, with criminal records and violent attitudes, thus dealing with specific aspects of a matter that already then was of great public concern… The punishment of a journalist for assisting in the dissemination of statements made by another person in an interview would seriously hamper the contribution of the press to discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so."[221]

Building counter-narratives as a response to hate speech

According to the United Nations Educational, Scientific and Cultural Organization (UNESCO), non-legal methods of countering hate speech are as important as legal proscriptions. One such measure is building a counter-narrative by promoting greater media and information literacy as a structural response to hate speech online:

> "Given young people's increasing exposure to social media, information about how to identify and react to hate speech may become increasingly important. It is particularly important that anti-hate speech modules are incorporated in those countries where the actual risk of widespread violence is highest. There is also a need to include in such programmes, modules that reflect on identity, so that young people can recognise attempts to manipulate their emotions in favour of hatred, and be empowered to advance their individual right to be their own masters of who they are and wish to become."[222]

[221] European Court of Human Rights, Application No. 15890/89, (1994) para. 33-35 (accessible at: http://hudoc.echr.coe.int/eng?i=001-57891).
[222] UNESCO, Iginio Gagliardone et al, 'Countering online hate speech' at p 58 (accessible at: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf).

MUST VIOLENCE OR HATRED ACTUALLY RESULT?

Another tenet of the Rabat Plan of Action threshold test is the likelihood and imminence of harm.[223] Incitement, by definition, is an inchoate crime. The action advocated through incitement speech does not have to be committed for it to amount to a crime. Nevertheless, some degree of risk of resulting harm must be identified. This means that courts will have to determine that there was a reasonable probability that the speech would succeed in inciting violence, discrimination or hostility against the target group. Courts in different jurisdictions have differed on just how likely the harm needs to be to constitute a criminal act.

For example, in *Devgan v. Union of India*,[224] the Supreme Court of India interpreted sections 295A and 505 of the Penal Code, which proscribe "deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs" and "statements conducing to public mischief", including "Statements creating or promoting enmity, hatred or ill-will between classes", as well as section 153A, which prohibits promoting "enmity between different groups on grounds of religion, race, place of birth, residence, language etc. and doing acts prejudicial to the maintenance of harmony." The Court provided the following guidance regarding the required likelihood of actual harm resulting from speech:

> [55]: "Sometimes, difficulty may arise and the courts … would have to exercise discernment and caution in deciding whether the 'content' is a political or policy comment, or creates or spreads hatred against the targeted community … The 'content' should reflect hate which tends to vilify, humiliate and incite hatred or violence against the target group based upon identity of the group beyond and besides the subject matter."
>
> …
>
> [67]: "Clauses (a) and (b) to sub-section (1) to Section 153A of the Penal Code use the words 'promotes' and 'likely' respectively. Similarly, Section 295-A uses the word 'attempts' and … Section 505 uses the words 'create or promote.' Word 'likely' … convey[s] the meaning, that the chance of the event occurring should be real and not fanciful or remote … The standard of 'not improbable' is too weak and cannot be applied as it would infringe upon and fall foul of reasonable restriction and the test of proportionality…'Promote' does not imply mere describing and narrating a fact, or giving opinion criticising the point of view or actions of another person – it requires that the speaker should actively incite the audience to cause public disorder. This active incitement can be gauged by the content of the speech, the context and surrounding circumstances, and the intent of the speaker. However, in case the speaker does not actively incite the descent into public disorder, and is merely pointing out why a certain person or group is behaving in a particular manner, what are their demands and their point of view, or when the speaker interviews such person or group, it would be a passive delivery of facts and opinions which may not amount to promotion.
>
> [68]: "The word 'attempt', though used in Sections 153-A and 295-A of the Penal Code, has not been defined. However, there are judicial interpretations that an 'attempt to constitute a crime' is an act done or forming part of a series of acts which would constitute its actual commission but for an interruption. An attempt is short of actual causation of crime and more than mere preparation."

---

[223] OHCHR above n 3.

[224] *Devgan v. Union of India*, Writ Petition NO. 160 of 2020, 2020 SCC OnLine SC 994 (2020) (accessible at: https://indiankanoon.org/doc/179868451/).

Online hate speech laws being used to stifle free speech

Many states are increasingly resorting to new online hate speech laws with the stated goal of curbing the flood of mis- and disinformation that has been amplified with the advent of the internet and especially social media. For example, in 2018, Bangladesh passed the Digital Security Act[225] following sectarian violence fuelled by Facebook posts. However, many sections of this Act are worded in a vague and excessively broad manner, inconsistent with international standards on freedom of speech, including the requirements of legality and proportionality and necessity.[226] For example, section 25(a) of the Act criminalises the transmission, publication or propagation through websites or other digital media "any data-information which he knows to be offensive, false or threatening in order to annoy, insult, humiliate or malign a person."

Many online speech laws pose a risk to freedom of expression due to the following:

- Overly broad definitions of hate speech and disinformation.
- Vague provisions that allow for discretionary interpretation by law enforcers such as prosecutors and the police and enable the laws to be employed in a manner which is inconsistent with fundamental rights.
- Requiring internet intermediaries to police content.
- Providing for overly harsh and punitive penalties for violations.

THE DANGER OF VAGUENESS

The obvious danger in regulating hate speech is that vagueness in the definition of what constitutes a criminal speech act will be used to penalise expression that has neither the intent nor the realistic possibility of inciting hatred.

An example of a vague hate speech provision is section 298 of Singapore's Penal Code,[227] which proscribes various acts undertaken with the intention of hurting others' feelings, as opposed to requiring incitement to discrimination, hostility or violence. This section reads: "Whoever, with deliberate intention of wounding the religious or racial feelings of any person, utters any word or makes any sound in the hearing of that person, or makes any gesture in the sight of that person, or places any object in the sight of that person, or causes any matter however represented to be seen or heard by that person, shall be punished with imprisonment for a term which may extend to 3 years, or with fine, or with both."

[225] S.R.O. NO. 310-Law/2019 (accessible at: https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf).
[226] For an overview, see Centre for Law and Democracy, 'Bangladesh: Analysis of the Draft Digital Security Bill, (2018) (accessible at: https://www.law-democracy.org/live/bangladesh-digital-security-bill-seriously-flawed/).
[227] Penal Code of 1871 (revised 2020) (accessible at: https://sso.agc.gov.sg/act/pc1871).

ADVOCACY OF GENOCIDE OR HOLOCAUST DENIAL: SPECIAL CASES?

Some commentators argue that the issues of advocacy of genocide or denial of the Holocaust constitute special cases within the debate on hate speech and incitement. According to the 1948 Genocide Convention, "direct and public incitement to commit genocide" is a punishable act,[228] following the role of the media in perpetuating hatred against Jewish people in Germany and advocating for their extermination.

Likewise, in Rwanda the media played a crucial role during the genocide in drumming up hatred and distributing propaganda, which led to the first prosecutions at the International Criminal Tribunal for Rwanda (ICTR) for "direct and public incitement to commit genocide." In the same way as hate speech, incitement to genocide was defined as an inchoate crime, meaning it is not necessary for genocide to have actually occurred for the crime to have been committed, but it did require intent.

The most notable case brought against journalists at the ICTR was *Nahimana et al*, known as the Media Trial.[229] Two of the respondents were the founders of a radio station that broadcast anti-Tutsi propaganda before the genocide and the names and licence plate numbers of intended victims during the genocide.[230] They were convicted, among other things, of persecution, one of the acts which makes up crimes against humanity, for disseminating hate speech.[231]

The Rome Statute establishing the International Criminal Court also establishes the crime of incitement to genocide.[232]

The genocide of the Jews in Nazi-occupied Europe was such a formative event in the creation of the European human rights system that Holocaust denial — claiming that the genocide did not occur — is an offence in several countries and is treated in a particular fashion within the jurisprudence of the European Court of Human Rights.[233] These decisions reflect the particularly sensitive issue of the historical memory of the Holocaust in many European countries and the application of the European Court of Human Rights' 'margin of appreciation' doctrine, whereby Council of Europe member states are afforded some discretion on certain issues. However, from a principled perspective, Holocaust denial prohibitions raise human rights concerns. First, they may be considered discriminatory in that they single out a single genocide. Second, should engaging in revisionism amount to hate speech in a given context, it is unclear why dedicated genocide denial laws would be necessary to prosecute these offences instead of applying general hate speech provisions. And, should revisionism not amount to hate speech, it is very questionable whether it should be prohibited at all.

---

[228] United Nations General Assembly, Convention on the Prevention and Punishment of the Crime of Genocide, Resolution 260 (III) (1948), Art. 3.(accessible at: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf).
[229] International Criminal Tribunal for Rwanda, Case No. ICTR-99-52-T, (2003) (accessible at: https://unictr.irmct.org/en/cases/ictr-99-52).
[230] Media Defence above n. 2.
[231] Note 12, para. 1072.
[232] International Criminal Court, 'Rome Statue of the International Criminal Court' at articles 6, 25 and 33 (2002) (accessible at: https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf).
[233] For example, see the case of *Garaudy v. France*, Application No. 65831/01 (2003) at the ECtHR.

The growth of social media platforms has raised new concerns about the proliferation of incitement to genocide and other forms of hate speech. Facebook has come under criticism for its role in allegedly fuelling the spread of hateful content against the Rohingya minority in Myanmar through its failure to take sufficiently effective measures to remove hateful posts, a situation partially caused by the company's having had insufficient numbers of moderators and fact-checkers familiar with the situation in Myanmar and proficient in Burmese.[234] Another concern is Facebook's alleged role in amplifying hate speech through its algorithms, which prioritise sensational content.[235] Facebook's role in the violence against the Rohingya was referenced in a report by a UN Human Rights Council-authorised fact finding mission on Myanmar:

> 74. The role of social media is significant. Facebook has been a useful instrument for those seeking to spread hate, in a context where, for most users, Facebook is the Internet. Although improved in recent months, the response of Facebook has been slow and ineffective. The extent to which Facebook posts and messages have led to real-world discrimination and violence must be independently and thoroughly examined. The mission regrets that Facebook is unable to provide country-specific data about the spread of hate speech on its platform, which is imperative to assess the adequacy of its response.[236]

Facebook's role may come under judicial scrutiny because of class action filed in the US against Meta and a letter of notice filed in the United Kingdom by Rohingya refugees.[237]

DEFAMATION OF RELIGIONS

Many states in South and Southeast Asia have laws prohibiting defamation of religions, and many also have the crime of blasphemy. For example, Sri Lanka's Penal Code prohibits certain expressions which harm the 'religious feelings' of others.[238] In Indonesia it is prohibited to promote atheism or any religion other than the six enumerated under domestic law.[239] Some countries have implemented particularly harsh penalties for the crimes of blasphemy and defamation of religion, including death. For example, in Pakistan, blasphemy is a capital offence.[240]

---

[234] See Letter of Notice from McCue Jury & Partners to Meta on behalf of the Rohingya community living in the United Kingdom and Bangladesh (2021) (accessible at: https://rohingya-data.s3.amazonaws.com/attachments/ckwunsg221v4vgir2r34oysu6-roh-00352-fac-cor-ipc-2021-12-06-letter-of-notice-vf-26.pdf).
[235] Id. See also Global Witness, 'Algorithm of harm: Facebook amplified Myanmar military propaganda following coup' (2021) (accessible at: https://www.globalwitness.org/en/campaigns/digital-threats/algorithm-harm-facebook-amplified-myanmar-military-propaganda-following-coup/).
[236] UN Human Rights Council, 'Report of the independent international fact-finding mission on Myanmar', A/HRC/39/64 (2018) (accessible at: https://www.ohchr.org/en/hr-bodies/hrc/myanmar-ffm/reportofthe-myanmar-ffm).
[237] Ram Eachambadi, Jurist, 'US and UK Rohingya refugees sue Facebook alleging dissemination of "hateful and dangerous misinformation"' (2021) (accessible at: https://www.jurist.org/news/2021/12/us-and-uk-rohingya-refugees-sue-facebook-alleging-dissemination-of-hateful-and-dangerous-misinformation/).
[238] End Blasphemy Laws, 'Sri Lanka' (2021) (accessible at: https://end-blasphemy-laws.org/countries/asia-central-southern-and-south-eastern/sri-lanka/).
[239] End Blasphemy Laws, 'Indonesia' (2020) (accessible at: https://end-blasphemy-laws.org/countries/asia-central-southern-and-south-eastern/indonesia/).
[240] End Blasphemy Laws, 'Pakistan' (2020) (accessible at: https://end-blasphemy-laws.org/countries/asia-central-southern-and-south-eastern/pakistan/).

These laws represent a breach of the right to freedom of expression. General Comment 34 states that:[241]

> "Prohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the Covenant, except in the specific circumstances envisaged in article 20, paragraph 2, of the Covenant. Such prohibitions must also comply with the strict requirements of article 19, paragraph 3, as well as such articles as 2, 5, 17, 18 and 26. Thus, for instance, it would be impermissible for any such laws to discriminate in favour of or against one or certain religions or belief systems, or their adherents over another, or religious believers over non-believers. Nor would it be permissible for such prohibitions to be used to prevent or punish criticism of religious leaders or commentary on religious doctrine and tenets of faith."

Many other countries have abolished the offence of blasphemy in recent years, for example the United Kingdom in 2008,[242] Denmark in 2017, [243] and Canada in 2018.[244]

CONCLUSION

Hate speech is a highly contentious issue in South and Southeast Asia, dividing the community of freedom of expression defenders on where the line should be drawn between protecting speech that is harmful to minority groups and enabling important dissent and criticism. The challenges of dealing with hate speech are particularly salient in online hate speech cases, where the notion of intent can be complicated and remedies harder to implement. Defamation of religions and blasphemy laws should be removed from criminal statutes. While prohibitions on incitement to particularly tragic past events such as genocides are legitimate, there are questions as to whether prohibitions on merely denying genocides, or specific prohibitions on denial of the Holocaust, are justified.

---

[241] UN Human Rights Council, 'General Comment No. 34 at p 12 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[242] Media Defence, 'Training Manual on International and Comparative Media and Freedom of Expression Law', Richard Carver, (2020) (accessible at: https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-international-and-comparative-media-and-freedom-of-expression-law/).
[243] The Guardian, 'Denmark scraps 334-year old blasphemy law' (2017) (accessible at: https://www.theguardian.com/world/2017/jun/02/denmark-scraps-334-year-old-blasphemy-law).
[244] Global News Wire, 'Repeal of Canada's Blasphemy Law Applauded by National Secularist Organization' (2018) (accessible at: https://www.globenewswire.com/news-release/2018/12/14/1667079/0/en/Repeal-of-Canada-s-Blasphemy-Law-Applauded-by-National-Secularist-Organization.html).

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.[245] 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 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.

[245] 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).

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."[246]

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.[247] 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.[248]

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.[249]

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."[250]

---

[246] 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).
[247] 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).
[248] *Id.*
[249] ITU Definition of Cybersecurity, (accessible at: https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx).
[250] 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.[251] 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.[252] 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.[253]

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.[254]

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.[255]

---

[251] Council of Europe, 'Budapest Convention and Related Standards', (accessible at: https://www.coe.int/en/web/cybercrime/the-budapest-convention).
[252] 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).
[253] 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).
[254] 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).
[255] 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.[256] However, many states continue to protect individuals' privacy only inadequately, especially from state surveillance activities.[257]

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*[258] 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.[259]

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".[260]

---

[256] 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).

[257] 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).

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

[259] *Id.* at para 21.

[260] *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.[261] 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.[262] When afforded opportunities to file a further affidavit, the Solicitor General declined, citing national security concerns as the reason for not revealing further information.[263]

The Supreme Court of India reaffirmed its previous holding in *Puttaswamy*[264] that privacy was 'sacrosanct'[265] 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."[266] 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.[267] The Court further noted the case's significance for the protection of journalistic sources.[268]

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.[269] 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."[270] 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.[271]

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.*[272] 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

[261] 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/).
[262] *Manohar*, n 14 at para 12.
[263] *Id.* at paras. 13-17.
[264] *K.S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012 (2018) (accessible at: https://indiankanoon.org/doc/127517806/).
[265] Manohar, n 14 at para. 32.
[266] *Id.* at para. 52.
[267] *Id.* at para. 39.
[268] *Id.* at paras. 40-41.
[269] *Id.* at paras 46 and 51.
[270] *Id.* at para 49.
[271] *Id.* at paras 54-55.
[272] G.R. No. 203335 (2014) (accessible at: https://lawphil.net/judjuris/juri2014/feb2014/gr_203335_2014.html).

Act" was deemed 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.[273] 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.[274]

[273] 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).
[274] 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.[275]

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.[276]

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.[277] 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."[278]

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.[279]

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.

---

[275] Article 19, 'Freedom of Expression and ICTs' (2018) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf).
[276] 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).
[277] *Id.* at para. 71.
[278] 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.)
[279] 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.[280] Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.[281]

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.[282] The Philippines[283] and Singapore[284] 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.[285] 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

[280] Pew Research Center, 'Online harassment 2017, (2017), (accessible at: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/).
[281] *Id.*
[282] 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).
[283] *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).
[284] 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).
[285] 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.[286] Lastly, the term oversimplifies the offence by ignoring a range of aggressors and motivations and invoking a moralist reaction against the victim.[287]

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."[288]

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.[289]

Cyberbullying Legislation in the Philippines

The Philippines has sought to address cyberbullying among children through the Anti-Bullying Act of 2013.[290] 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),

---

[286] *Id.*
[287] 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)).
[288] UNICEF, 'Cyberbullying: What is it and how to stop it' (accessible at: https://www.unicef.org/end-violence/how-to-stop-cyberbullying).
[289] 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).
[290] 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.[291]

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."[292] 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,[293] a series of principles

[291] 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.
[292] 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).
[293] 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[294] and subsequently endorsed in a UN General Assembly resolution.[295]

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.[296] Cambodia, Myanmar and the Maldives are currently in the process of drafting such legislation.[297]

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.[298] 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.[299] 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."[300]

STEPS TO TAKE IN RESPONSE TO ONLINE HARMS

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

---

[294] 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).
[295] 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).
[296] United Nations Conference on Trade and Development, 'Cybercrime Legislation Worldwide' (2021) (accessible at: https://unctad.org/page/cybercrime-legislation-worldwide).
[297] *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).
[298] 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/).
[299] 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).
[300] *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).[301]
- **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.[302]

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

[301] 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/).
[302] 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.

MODULE 8: 'FALSE NEWS', MISINFORMATION AND PROPAGANDA

- **'False news' refers to news items that are intentionally and verifiably false, and seek to mislead readers. Disinformation is any information that is spread in the knowledge that it is false. Misinformation is false information that is spread but where the person who is responsible for that does not know that it is false.**

- **While acknowledging the social ills may be occasioned by false news and misinformation, courts and international standards indicate that general provisions which criminalise false news and misinformation violate the right to freedom of expression.**

- **As a result, strategies to combat dis- and misinformation, need to be more social and educational in their character. These include media and information literacy (MIL) strategies and campaigns which focus on human rights, media, digital, intercultural, and privacy literacy as a holistic method of mitigating the impact of dis- and misinformation. These strategies may be complemented by social media verification, fact-checking, and the prioritisation of reliable content and the publication of counter-narratives.**

- **In limited instances, dis- and misinformation may constitute hate speech, the dissemination of which may be criminal in nature. However, any litigation relating to expression should be fully considered for unintended consequences and the possibility of impacts which may undermine freedom of expression.**

- **Propaganda for war is dissimilar to dis- and misinformation in that international law expressly calls for it to be prohibited.**

INTRODUCTION[303]

The phenomenon of false news and misinformation has increased exponentially in recent times with the advent of the internet and social media platforms. While manipulating and distorting information is squarely part of the historical record, the weaponisation of information in the 21st century is occurring on an unprecedented scale, which requires urgent and effective responses. This module focuses on 'false news', misinformation and propaganda, and provides guidance on media and information literacy (MIL) strategies and campaigns[304] which may assist with mitigating dis- and misinformation while ensuring that the right to freedom of expression is not violated.

[303] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-digital-rights-and-freedom-of-expression-online/). For further information see First Draft, 'Understanding and addressing the disinformation ecosystem' (2017) (accessible at: https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v3.pdf?x17007).
[304] *Id* at page 70 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000265552).

WHAT IS 'FALSE NEWS'

'False news' refers to news items that are intentionally and verifiably false, and seek to mislead readers. In March 2017, the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda (2017 Joint Declaration) was issued by the relevant freedom of expression mandate-holders of the United Nations (UN), the African Commission on Human and Peoples' Rights (ACHPR), the Organisation for Security and Co-operation in Europe (OSCE), and the Organisation of American States (OAS).[305] The 2017 Joint Declaration noted the growing prevalence of disinformation and propaganda, both online and offline, and the various harms to which they may contribute or be a primary cause. The quandary remains that the internet, and especially social media platforms, both facilitate the circulation of disinformation and propaganda and also provides a useful tool to enable responses to this.

Importantly, the 2017 Joint Declaration stressed that general prohibitions on the dissemination of information based on vague and ambiguous ideas, such as "false news", are incompatible with international guarantees of freedom of expression. However, it went further to state that this did not justify the dissemination of knowingly or recklessly false statements by state actors. In this regard, the Joint Declaration called on state actors to take care to ensure that they disseminate reliable and trustworthy information, and not to make, sponsor, encourage or further disseminate statements that they know (or reasonably should know) to be false or which demonstrate a reckless disregard for verifiable information.

The 2017 Joint Declaration identified the following standards on disinformation and propaganda:

> "Standards on disinformation and propaganda
>
> (a) General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.
>
> (b) Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.
>
> (c) State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).
>
> (d) State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest, such as the economy, public health, security and the environment."

False news provisions are legal rules which prohibit and punish the dissemination of false or inaccurate statements. Such rules have not be put in place in many countries. However, recently certain governments have introduced new false news prohibitions, a worrying trend

[305] Accessible at: https://www.osce.org/fom/302796?download=true.

that gathered speed following the onset of the COVID-19 pandemic and the imposition of emergency measures, sometimes under the pretext of combatting medical disinformation or panic. In July 2021, amidst a state of emergency that had been declared in response to the pandemic, the Thai government enacted, pursuant to an emergency decree, Regulation 29, which criminalised the dissemination of texts that may "instigate fear" or are "intended to distort information to mislead understanding of the emergency situation to the extent of affecting the security of state or public order or good morals of the people."[306] The Regulation was met with alarm by human rights organisations which viewed it as inconsistent with Thailand's international obligations, including the requirements that restrictions on freedom of expression under the ICCPR be provided by law, necessary and proportionate, and pursue a legitimate aim.[307]

The media company Reporter Production sought an order halting the enforcement of the Regulation pursuant to which the Civil Court granted the application. In reasons for the order, the Court found Article 1 of the Regulation, prohibiting the dissemination of information that may instigate fear, to be inconsistent with the guarantee of freedom of expression as contained in the Thai Constitution. The Court further noted the vagueness of the article, expressing concerns about the chilling effect it would have on the media:

> Moreover, the phrase "information having a risk of frightening people" as indicated in such Article is of an ambiguous character and opens a possibility to a broad interpretation, thereby rendering the plaintiffs, people and those working in media field unconfident about expressing their opinion and communicating in accordance with the freedom protected by Article 34 Paragraph 1, Article 35 Paragraph 1 of the Constitution. Such Article results in a superfluous and unnecessary deprivation of people's right and freedom, which makes it, in effect, incompatible with Article 26 Paragraph 1 of the Constitution.[308]

MISINFORMATION, DISINFORMATION AND MAL-INFORMATION

The problem statement

Misinformation is anathema to quality of journalism and the circulation of trustworthy information which complies with professional standards and ethics.[309] However, dis- and misinformation are not new but rather have become increasingly prevalent as they are fuelled by new technologies and rapid online dissemination of communications. The

[306] Joint Statement of Access Now *et. al.*, "Thailand: Immediately repeal emergency regulation that threatens online freedoms" (2021) (accessible at: https://www.hrw.org/sites/default/files/media_2021/08/210803%20Thailand%20Regulation%20No.%2029%20Joint%20Statement.pdf).
[307] *Id.*
[308] Order in *Reporter Production Co., Ltd et al. v. Thailand's Prime Minister Prayut Chan-o-cha* (2021) (accessible at: https://civil.coj.go.th/cms/s41/u392/6408/PR640806en.pdf).
[309] UNESCO, 'Journalism, Fake News & Disinformation' (2018) at p.18 (accessible at https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf.

consequence is that digitally-fuelled dis- and misinformation, especially in contexts of polarisation, risks eclipsing quality journalism, and the truth.[310]

Increasingly, the strategies to combat dis- and misinformation are more social, educational and technical in their character in order to ensure that the right to freedom of expression is not violated by over-broad legislative provisions which criminalise this sort of speech. Addressing the dis- and misinformation ecosystem, therefore, requires a critical assessment of the reasons for the dissemination of this sort of content and the establishment of MIL campaigns.[311] In effect, combatting dis- and misinformation, at this stage, falls more within the realm of advocacy and education than it does litigation. The limited litigation in this space bears testament to this. However, this is likely to change as digital rights litigators engage in more strategic and test case litigation seeking to mitigate dis- and misinformation while protecting and promoting freedom of expression.

Defining false information[312]	
Disinformation	Disinformation is information that is false, and the person who is disseminating it knows it is false. "It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors".[313]
Misinformation	Misinformation is information that is false, but the person who is disseminating is not aware that it is false.[314]
Mal-information	Mal-information is information that is based on reality but it is used to inflict harm on a person, organisation or country.[315]

Causes of dis- and misinformation

To understand how to combat dis- and misinformation, it is useful to first understand how it spreads. With the advent of the information age and the internet, information is spread more rapidly, often with the click of a mouse.[316] Equally, the speed at which information is transmitted and the instant access to information which the internet provides has caused a rush to be the first to publish information, as well as the often thoughtless retransmission or promotion of the statements of others. This, alongside more insidious practices such as the intentional distribution of disinformation for economic or political gain, has created what the UN Educational, Scientific and Cultural Organisation (UNESCO) refers to as a "perfect storm".[317]

---

[310] *Id.*
[311] *Id* at p. 70.
[312] *Id* at pp. 45-6.
[313] *Id* at pp 44-5.
[314] *Id.*
[315] *Id.*
[316] *Id* at p.55.
[317] *Id.*

UNESCO identifies three causes enabling the spread of dis- and misinformation:

1. **Collapsing traditional business models.** The rapid decline in advertising revenue and the migration of advertising to digital actors means that traditional newsrooms have far less resources. This, in turn, has led to reduced quality news and less time for "checks and balances". It also promotes "click-bait" journalism.[318] As a result, legacy media is bleeding audiences, with media consumers moving to "peer-to-peer" news products offering "on demand-access". Importantly, peer-to-peer news has no agreed-upon ethics and standards.
2. **Digital transformation of newsrooms and storytelling.** As the information age develops, there is a discernible digital transformation in the news industry. This transformation causes journalists to prepare content for multiple platforms, limiting their ability to properly interrogate facts. Often, journalists apply a principle of "social-first publishing" whereby their stories are posted directly to social media to meet audience demand in real-time. This, in turn, promotes click-bait journalism and the pursuit of "virality" as opposed to quality and accuracy.[319]
3. **The creation of new news ecosystems.** With increasing access to social media platforms, users can curate their own content streams and create their own "trust networks" or "echo chambers" within which inaccurate, false, malicious and propagandistic content can spread. These new ecosystems allow dis- and misinformation to flourish as users are more likely to share "exciting" or sensationalist stories and are far less likely to properly assess sources or facts. Importantly, once disseminated, a user who becomes aware that a statement may constitute misinformation is largely unable to "pull back" or correct it.[320]

These causes continue to pose difficulties for newsrooms, journalists, and social media users as the new news ecosystems, in particular, enable malicious practices and actors to flourish. However, as discussed, there is a fine line between seeking legitimate ways to combat the spread of dis- and misinformation online and violating the right to freedom of expression.

WASHLITE v Fox News[321]

On 2 April 2020, the Washington League for Increased Transparency and Ethics (WASHLITE) instituted proceedings against Fox News, a right-wing American news network, claiming that "Fox's repeated claims that the COVID-19 pandemic was/is a hoax is not only an unfair act, it is deceptive and therefore actionable under Washington's Consumer Protection Act."[322] WASHLITE sought a declaration to this effect and an injunction (interdict) prohibiting repeated statements on Fox News stating that COVID-19 is a hoax. In its findings, the Washington Superior Court found that WASHLITE's goal

[318] *Id* at p. 57.
[319] *Id* at pp. 57-8.
[320] *Id* at pp. 59-61.
[321] *Washington League for Increased Transparency and Ethics v Fox News*, Plaintiffs Complaint for Declaratory and Injunctive Relief, 2 April 2020 (accessible here: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3190&context=historical).
[322] *Id.*

was "laudable" but that its arguments ran "afoul of the protections of the First Amendment", which guarantees right to freedom of expression, and hence dismissed the case.

How to combat dis- and misinformation

Effectively combatting dis- and misinformation remains a pressing contemporary issue, with various remedies posited by jurists, academics, and activists. Notably, Justice Anthony Kennedy of the United States Supreme Court, in his majority decision in *United States v Alvarez*[323] held: "The remedy for speech that is false is speech that is true. This is the ordinary course in a free society. The response to the unreasoned is the rational; to the uninformed, the enlightened; to the straight-out lie, the simple truth."[324] MIL strategies and campaigns proposed by UNESCO seek to operationalise the position proposed by Justice Kennedy and provide a holistic approach to combating dis- and misinformation, without limiting the right to freedom of expression.

STRATEGIES TO ADDRESS "FALSE NEWS"

Media and Information Literacy (MIL) Strategies and Campaigns

As a point of departure, UNESCO proposes MIL strategies and campaigns as a process which enables the detection and mitigation of dis- and misinformation and a means to combat its spread, particularly online.[325] MIL is an umbrella and inter-related concept which encompasses the following ideas:

- **Human rights literacy** which relates to the fundamental rights afforded to all persons, including the right to freedom of expression, and the promotion and protection of these fundamental rights.[326]
- **News literacy** which refers an understanding of the news media, including journalistic standards and ethics.[327] This includes, for example, the ability to understand the "language and conventions of news as a genre and to recognise how these features can be exploited with malicious intent."[328]
- **Advertising literacy** which refers to understanding how advertising online works and how profits are driven in the online economy.[329]
- **Computer literacy** which refers to basic IT usage and understanding the easy manner in which headlines, images, and, increasingly, videos can be manipulated to promote a particular narrative.[330]
- **Understanding the "attention economy"**, which is one of the causes of dis- and misinformation, based on pressure on journalists and editors to focus on click-bait headlines

[323] *United States v Alvarez*, 567 U.S. 709 (2012) (accessible at: https://www.supremecourt.gov/opinions/11pdf/11-210d4e9.pdf).
[324] *Id* at pp. 15-6.
[325] UNESCO Handbook, above n 7 at p.70).
[326] *Id* at p.70.
[327] *Id.*
[328] *Id.*
[329] *Id.*
[330] *Id.*

and misleading imagery to grab the attention of users and, in turn, drive online advertising revenue.[331]

- **Privacy and intercultural literacy** which relates to understanding standards on the right to privacy and a broader understanding of how communications interact with induvial identity and social developments.[332]

MIL strategies and campaigns, such as the COVID-19 campaign by the UN detailed below, should underscore the importance of media and information literacy in general but should also include a degree of philosophical understanding. According to UNESCO, "[MIL strategies and campaigns should assist users] grasp that authentic news does not constitute the full 'truth' (which is something only approximated in human interactions with each other and with reality over time)."[333]

"Five ways the UN is fighting 'infodemic' of misinformation"[334]

The COVID-19 pandemic has generated significant amounts of dis- and misinformation, ranging from allegations about how to use disinfectants to combat the virus to false claims that the virus can spread through radio waves and mobile networks. In order to counter this "infodemic", the UN has taken five steps:

1. **Produce and disseminate facts and accurate information.** The UN identified the World Health Organisation (WHO) as the lead agency in the battle against the pandemic, responsible for transmitting authoritative information based on science while also seeking to counter myths. Identifying sources such as the WHO that produce and disseminate facts is a central tenet to countering dis- and misinformation.
2. **Partner with platforms and suitable partners.** Allied to the distribution of accurate information is finding the right partners. The UN and the WHO have partnered with the International Telecommunications Union (ITU) and the UN Children's Fund (UNICEF) to help persuade all telecommunications companies worldwide to circulate factual text messages about the virus.
3. **Work with the media and journalists.** UNESCO has published two policy briefs that assess the COVID-19 pandemic which assist journalists working on the frontlines of the "infodemic" around the world to provide accurate, trustworthy and verifiable public health information.
4. **Mobilise civil society.** Through the UN Department of Global Communications, key information on opportunities to access, participate and contribute to UN processes during COVID-19 have been communicated to civil society organisations (CSOs) to help ensure that all relevant stakeholders ae connected.
5. **Speak out for rights.** Michelle Bachelet, the UN High Commissioner for Human Rights, recently joined a chorus of other activists, to speak out against restrictive measures imposed by states against independent media, as well as the arrest and intimidation of journalists, arguing that the free flow of information is vital in fighting COVID-19.

---

[331] *Id* at p.47.
[332] *Id* at p.70.
[333] *Id* at p.72.
[334] Accessible at: https://www.un.org/en/un-coronavirus-communications-team/five-ways-united-nations-fighting-%E2%80%98infodemic%E2%80%99-misinformation.

Litigation Where Justifiable Limitations Exist[335]

The International Covenant on Civil and Political Rights (ICCPR) provides in article 20 that "propaganda for war shall be prohibited by law" and that "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."

In addition, article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination (CERD) requires that the dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, must be declared an offence that is punishable by law.

Despite the importance of freedom of expression, not all speech is protected under international law, and some limited types of speech are required to be prohibited by states. However, there is a need for clear and narrowly circumscribed definitions of what is meant by the term "hate speech", and objective criteria that can be applied. Over-regulation of hate speech can violate the right to freedom of expression, while under-regulation may lead to discrimination, harassment or violence against minorities and protected groups.

In instances where dis- and misinformation is so egregious that it meets the definitional elements of hate speech, prosecutions may be a useful and important tool in the protection and promotion of fundamental rights, includes the right to equality and dignity.[336] However, such litigation should be fully considered for unintended consequences and the possibility of jurisprudence which may negatively impact freedom of expression. Depending on the content of the speech and the harm that it causes, the publication of counter-narratives may constitute a useful complementary strategy to litigation.

For more information on this topic, see module 6 of this series.

Fact-checking and Social Media Verification

Alongside MIL strategies and campaigns and prosecuting instances of hate speech, another effective tool to combat dis- and misinformation is fact-checking and social media verification. According to the Duke Reporters' Lab, in 2021 there were over 391 fact-checking projects debunking false news and misinformation in more than 100 countries, a sizeable increase from 186 projects in 2016, although the rate of growth has been slowing.[337]

In general, fact-checking and verification processes, which were first introduced by US weekly magazines such as *Time* in the 1920s,[338] consist of:

---

[335] See Module 6 of this series for more information on hate speech and justifiable limitations to freedom of expression.
[336] For a useful discussion on the balancing of rights see T. Mendel, *Study on International Standards Relating to Incitement to Genocide or Racial Hatred*, 2006 (accessible at: http://www.concernedhistorians.org/to/239.pdf).
[337] Duke Reporters' Lab, 'Fact-checkers extend their global reach with 391 outlets, but growth has slowed' (17 June 2022) (accessible at: https://reporterslab.org/fact-checkers-extend-their-global-reach-with-391-outlets-but-growth-has-slowed/).
[338] UNESCO Handbook above n 7 at p.81.

- **Ex-ante fact-checking and verification.** Increasingly and due to shrinking newsroom budgets, ex-ante (or before the event) fact-checking is reserved for more prominent and established newsroom and publications who employ dedicated fact-checkers.[339]
- **Ex-post fact-checking, verification and "debunking".** This method of fact-checking is becoming increasingly popular and focuses on checking information published after the fact. It concentrates "primarily (but not exclusively) on political ads, campaign speeches and political party manifestos" and seeks to make politicians and other public figures accountable for the truthfulness of their statements.[340] Debunking is a subset of fact-checking and requires a specific set of verification skills, increasingly in relation to user-generated content on social media platforms.

In addition to these tools, various other social media measures can be used. One which has attracted more attention recently is the prioritisation of verifiable content and deprioritisation of false content.

Fact-checking is central to strategies to combat dis- and misinformation and has grown exponentially in recent years due to the increasing spread of false news and misinformation, and the need to debunk viral hoaxes.[341] Alongside MIL strategies and campaigns, fact-checking and social media verification is becoming increasingly important in the fight against false news and misinformation.

Regional Initiatives to Address Disinformation and Misinformation

Since the outbreak of the COVID-19 pandemic, many states have resorted to combatting disinformation and misinformation through repressive means, contrary to international standards. For example, in March 2020, the Philippines enacted the *Bayanihan to Heal as One Act*, which declared the pandemic a national emergency and included a provision criminalising the spread of false information.[342] Similar anti-'fake news' criminal provisions were introduced in other states in Asia, including Vietnam,[343] Bangladesh[344] and Thailand.[345]

---

[339] *Id.*
[340] *Id* at p.82.
[341] For more resources on the legal defence of factcheckers, see the Fact-Checkers Legal Support Initiative (accessible at: https://factcheckerlegalsupport.org/).
[342] Republic Act No. 11469, section 6(f) (2020), (accessible at: https://pnl-law.com/blog/bayanihan-to-heal-as-one-act-republic-act-no-11469-full-text/); see also Jeremiah Joven B Joaquin and Hazel T Biana, 'Philippine crimes of dissent: Free speech in the time of COVID-19', *Crime Media Culture* Vol. 17(1) 37–41 (2021), (accessible at: https://journals.sagepub.com/doi/pdf/10.1177/1741659020946181).
[343] Reuters, Phuong Nguyen and James Pearson, 'Vietnam introduces 'fake news' fines for coronavirus misinformation'(2020), (accessible at: https://www.reuters.com/article/us-health-coronavirus-vietnam-security-idUSKCN21X0EB).
[344] 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).
[345] International Federation of Journalists, 'Thailand: New regulation curtails free speech' (2021) (accessible at: https://www.ifj.org/media-centre/news/detail/category/press-releases/article/thailand-new-regulation-curtails-free-speech.html).

Despite such worrying trends, there have been certain initiatives aimed at combatting disinformation and misinformation through non-repressive means. In January 2022, the Association of Southeast Asian Nations (ASEAN) Senior Officials Meeting on Education launched the *Training-of-Trainers Program to Counter Disinformation and Promote Media Literacy.*[346] This project focuses on the role of education in combatting disinformation and aims to provide resources to educators to enhance critical thinking among students regarding social media and the risks of disinformation.[347]

The Asia Internet Coalition, an industry group counting multiple major technology companies such as Meta (Facebook) and Google,[348] has also been advocating for non-censorship-based approaches to combatting disinformation. Initiatives by this coalition and other internet companies, sometimes in partnership with journalists and civil society, include "establishing and maintaining fact-checking programs, conducting research into the issue, and investing in the development and roll out of digital literacy training to millions of people in the region."[349]

PROPAGANDA

As detailed above and in module 6 of this series, unlike dis- and misinformation, the spread of propaganda for war is expressly prohibited in international law.[350] In these instances, direct legal remedies such as criminal prosecutions and interdictory or injunctive relief may result. However, often propaganda does not meet the threshold for such a legal response. In these instances, MIL strategies and campaigns and fact-checking, coupled with the publication of counter-narratives or counter-disinformation, can be effective remedies.[351]

CONCLUSION

The advent of the internet and the proliferation of false news and misinformation occasioned by the increased use of social media platforms is a primary contemporary concern. It fuels political polarisation and impacts a plethora of fundamental rights, including the right to freedom of expression, equality, and free and fair elections. However, outside of a narrow band of legitimately proscribable speech, the remedies to combat dis- and misinformation are, at this stage, largely social and educational. MIL strategies and campaigns, coupled with fact-checking and the publication of counter-narratives, remain the primary vanguard in the fight for the truth.

---

[346] Association of Southeast Asian Nations, 'New ASEAN initiative emphasises education as key to media literacy and countering disinformation' (2022) (accessible at: https://asean.org/new-asean-initiative-emphasizes-education-as-key-to-media-literacy-and-countering-disinformation/).
[347] *Id.*
[348] See Asia Internet Coalition, 'Members' (accessible at: https://aicasia.org/members/).
[349] The Diplomat, Jeff Paine, 'The Future of Asia's Battle Against Online Misinformation' (2021), (accessible at: https://thediplomat.com/2021/06/the-future-of-asias-battle-against-online-misinformation/).
[350] Article 20 of the ICCPR, read with article 4(a) of CERD.
[351] See, for example, the UK Government Communications Services, 'RESIST: Counter-disinformation toolkit' (accessible at: https://www.fundacioncarolina.es/wp-content/uploads/2020/11/Toolkit-UK.pdf.

MODULE 9: NATIONAL SECURITY

- **"National security" is a common justifications offered by states for limiting freedom of expression by journalists, bloggers, and media organs. However, it has the potential to be relied upon to quell dissent and cover up state abuses.**
- **National security legislation can have wide-reaching implications for media freedom and can be abused in ways that effectively avoid constitutional checks and balances.**
- **The Johannesburg and the Tshwane Principles, alongside the Siracusa Principles, provide guidance on the extent of the national security limitation in relation to media freedom and access to information although they only constitute non-binding international law.**
- **Recent instances of terrorism have caused international decision-makers to seek to better define terrorist activities in order to ensure that limitations of fundamental rights based on combatting terrorism are properly prescribed by law.**
- **There is a strong presumption that prior restraints on freedom of expression, even where imposed to protect national security, represent a breach of guarantees of this right, for example as set out in the precedent by the United States Supreme Court in the *Pentagon Papers* case.**

INTRODUCTION[352]

"National security" is a common justification offered by states for limiting freedom of expression by journalists, bloggers, and media organs. It is a legitimate ground for restricting freedom of expression in the International Covenant on Civil and Political Rights (ICCPR)[353].

Exceptionally, the right to freedom of expression can be partly suspended — a process known as *derogation* — in the case of a state of emergency due to a grave, imminent security threat. However, national security is often relied upon for illegitimate reasons, such as to quell dissent or to cover up state abuses.

This module examines how national security is treated under international and regional human rights law as a ground for limiting freedom of expression.

[352] This module should be read in conjunction with Richard Carver 'Training Manual on International and Comparative Media and Freedom of Expression Law at pp 76-86 (accessible here: https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-international-and-comparative-media-and-freedom-of-expression-law/)

[353] International Covenant on Civil and Political Rights (1966) at articles 19, 21 and 22 (accessible at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx).

THE DEROGATION PROCESS UNDER INTERNATIONAL

Most of the key human rights instruments allow a temporary derogation from certain human rights obligations in situations of national emergency. For example, article 4 of the ICCPR states:

> "In a time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin."[354]

Article 4 then proceeds to list a number of articles that may not be derogated from, even in times of public emergency. These include the rights not to be enslaved or tortured, and the right to freedom of opinion. It does not, however, include the right to freedom of expression.

The United Nations Human Rights Committee (UNHRCtte) has devoted two of its General Comments to explaining, in detail, the meaning of article 4 and the procedure and scope of derogation. The more recent of these, General Comment No. 29, can be taken as an authoritative interpretation of derogation during states of emergency. There are a number of key points to note:

- The state of emergency must be publicly proclaimed according to domestic legal requirements, and should also be accompanied by notification to other State Parties via the UN Secretary General or other body that serves as the technical secretariat of the treaty, explaining why it is necessary.[355]
- The situation leading to derogation must be "a public emergency which threatens the life of the nation."[356] In terms of General Comment No. 29, the threshold of threatening "the life of the nation" is a high one, and the UNHRCttee has been highly critical of derogations that have taken place in situations that appear to fall short of the article 4 requirements.[357]
- The UNHRCtte emphasises the importance of the principle that derogations should be limited "to the extent strictly required by the exigencies of the situation."[358] Even in instances where some form of derogation may be warranted, it should be limited to what is strictly required and necessary in the circumstances.

LIMITING MEDIA FREEDOM ON GROUNDS OF NATIONAL SECURITY

International law only allows the right to freedom of expression to be limited on grounds of national security where this is explicitly provided by law and the restriction is necessary and proportionate in an open and democratic society. In practice, however, national security is one of the most problematic areas of interference with media freedom.

---

[354] ICCPR above n 2 at article 4.
[355] United Nations Human Rights Council, 'General Comment No. 29, states of emergency (article 4)' at para. 2 (2001) (accessible at: https://digitallibrary.un.org/record/451555?ln=en).
[356] *Id.*
[357] *Id.* at para. 3.
[358] *Id.* at para. 4.

One difficulty is the tendency on the part of many governments to assume that it is legitimate to curb all public discussion on national security issues. Yet, according to international standards, expressions may only be lawfully restricted if they threaten actual damage to national security and if the restriction is necessary and proportionate to countering this threat.

In *Mat Shuhaimi bin Shafiei v. Malaysia*,[359] the Federal Court of Malaysia (the highest appellate court) ruled that a legislative provision criminalising sedition was unconstitutional after finding it to be a disproportionate restriction on freedom of expression and inconsistent with a constitutional guarantee of equality under the law. The sedition provision under review provided that the intention of the perpetrator was irrelevant.[360] The Court found this departure from general criminal law practice to constitute a disproportionate restriction on freedom of expression, noting that even more "socially abhorrent and heinous crimes" included, at a minimum, a rebuttable presumption that shifted the burden to the accused to disprove intent, as opposed to wholly displacing *mens rea* and creating a strict liability regime.[361]

The Johannesburg Principles

In 1995, a group of international experts met to discuss the Johannesburg Principles on Freedom of Expression and National Security.[362] Although non-binding, these principles are frequently cited (notably by the UN Special Rapporteur on freedom of expression) as a progressive summary of standards in this area. The Johannesburg Principles address the circumstances in which the right to freedom of expression might legitimately be limited on national security grounds, while also underlining the importance of the media, and freedom of expression and information, in ensuring accountability in the realm of national security.

In 2013, a group of civil society organisations from across the globe — including some who were involved in the drafting of the Johannesburg Principles — published an updated version, focusing on access to information, known as the 'Tshwane Principles.'[363] The Tshwane Principles state that:[364]

- Governments may legitimately withhold information in some narrowly defined areas, such as defence plans, weapons development, and the operations and sources used by intelligence services.

[359] Rayan Sivil No. W-01(A)-115-04/2015 (2016), (accessible at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/11/Mat-Shuhaimi-Shafiei-v-Kerajaan-Malaysia-Judgment-CoA.pdf).
[360] *Id.* at para 30.
[361] *Id.* at para 40.
[362] Article 19: Global Campaign for Free Expression, 'The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information,' (1996) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf).
[363]Open Society Justice Initiative, 'Understanding the Global Principles on National Security and the Right to Information' (2013) (accessible at: https://fas.org/sgp/library/tshwane-und.pdf).
[364] Open Society Justice Initiative, 'The Tshwane Principles on National Security and the Right to Information: An Overview in 15 Points' (accessible at: https://www.justiceinitiative.org/publications/tshwane-principles-national-security-and-right-information-overview-15-points#:~:text=Related%20Work-,The%20Tshwane%20Principles%20on%20National%20Security%20and%20the%20Right%20to,and%20national%20law%20and%20practices).

- Information about serious human rights violations may not be classified or withheld on national security grounds.
- People who disclose wrongdoing or other information of public interest (whistleblowers and the media) should be protected from any type of retaliation, provided they acted in good faith and followed applicable procedures.
- Disclosure requirements apply to all public entities, including the security sector and intelligence authorities.

Although the principles do not constitute binding international law, they were developed with wide consultation and have broad consensus; for example, they have been welcomed by all four of the special experts on freedom of expression — for the UN, the Organisation of American States (OAS), and the African Union (AU), and the Organisation for Security and Cooperation in Europe's (OSCE) expert on freedom of the media.[365]

THE SCOPE OF NATIONAL SECURITY

"Freedom of expression" and "national security" are very often seen as principles or interests that are inevitably opposed to each other. Governments often invoke national security as a rationale for restricting freedom of expression, particularly media freedom. Yet national security remains a genuine public good — and without it, media freedom would be scarcely possible. On the other hand, governments are seldom inclined to recognise that media freedom may actually be a means to ensure better national security by exposing abuses in the security sector.

The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR (Siracusa Principles) define a legitimate national security interest as one that aims "to protect the existence of the nation or its territorial integrity or political independence against force or threat of force."[366] Subsequent articles indicate that a national security limitation "cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order."

The UN Special Rapporteur on Freedom of Expression has repeatedly limited the scope of a national security limitation in similar terms. For example:

> "For the purpose of protecting national security, the right to freedom of expression and information can be restricted only in the most serious cases of a direct political or military threat to the entire nation."[367]

In a similar vein, the Johannesburg Principles define a national security interest as being:

---

[365] Open Society Justice Initiative above n 12.
[366] United Nations Economic and Social Council, 'Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights,' Principle 29 (1985) (accessible at: https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf).
[367] UN Special Rapporteur on Freedom of Expression, 'Report of the Special Rapporteur on the nature and scope of the right to freedom of opinion and expression, and restrictions and limitations to the right to freedom of expression,' (1995) (accessible at: https://www.ohchr.org/en/issues/freedomopinion/pages/annual.aspx).

> "To protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government."[368]

TERRORISM

Since the terror attacks in the United States on 11 September 2001, an important focus of security legislation has been on countering terrorism. In part, this reflects a genuine change in understanding the nature of threats to national security, seen also in the notion that terrorism or terrorist organisations are the objects of a "war." More generally, it serves as a rhetorical device whereby dissent — including critical media coverage — may be characterised as giving succour to terrorists.

The UN Security Council has required member states to take a number of steps to combat terrorism. One measure of particular relevance to the media is contained in Resolution 1624 of 2005, which was the first international instrument to address the issue of incitement to terrorism. The preamble to Resolution 1624 condemns "incitement to terrorist acts" and repudiates "attempts at the justification or glorification (*apologie*) of terrorist acts that may incite further terrorist acts."[369]

Defining terrorism

One serious problem with legal restrictions on glorification (or even incitement) of terrorism is the lack of any commonly accepted definition of terrorism in international law. Early counter-terrorism treaties focused on the criminalisation of particular acts, such as hijacking aircraft, without using the term terrorism. Later treaties, such as the International Convention for the Suppression of Financing of Terrorism,[370] do offer a definition, although this has no binding character beyond parties to the treaty.

Many states, as well as entities such as the European Union, define terrorism by reference to certain organisations "listed" as terrorist entities. This may hold particular dangers for the media in reporting the opinions and activities of such organisations, which they have a right to do. In their 2008 Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation,[371] the freedom of expression mandate-holders of the United Nations (UN), the African Commission on Human and Peoples' Rights (ACHPR), the Organisation for Security and Co-operation in Europe (OSCE), and the Organisation of American States (OAS) stated:

> "The public has a right to know about the perpetration of acts of terrorism, or attempts thereat, and the media should not be penalised for providing such information."[372]

---

[368] Johannesburg Principles above n 11 at Principle 2(a).
[369] UN Security Council, Resolution 1624 of 2005, (2005) (accessible at: http://unscr.com/en/resolutions/1624).
[370] International Convention for the Suppression of Financing of Terrorism, article 2(1) (1999)
[371] (2008) (accessible at: https://www.osce.org/files/f/documents/4/b/35639.pdf).
[372] *Id.*

The United Nations Special Rapporteur (UNSR) on counter-terrorism and human rights has offered a definition of terrorism, based upon best practices worldwide, which focuses on the act of terror rather than the perpetrator:[373]

> "Terrorism means an action or attempted action where:
>
> 1. The action:
>   a. Constituted the intentional taking of hostages; or
>   b. Is intended to cause death or serious bodily injury to one or more members of the general population or segments of it; or
>   c. Involved lethal or serious physical violence against one or more members of the general population or segments of it; and
> 2. The action is done or attempted with the intention of:
>   a. Provoking a state of terror in the general public or a segment of it; or
>   b. Compelling a Government or international organization to do or abstain from doing something; and
> 3. The action corresponds to:
>   a. The definition of a serious offence in national law, enacted for the purpose of complying with international conventions and protocols relating to terrorism or with resolutions of the Security Council relating to terrorism; or
>   b. All elements of a serious crime defined by national law."

Sometimes expression on its own is deemed a threat to national security — and these situations are addressed under incitement. For more detail on incitement, see Module 6 of this series on Hate Speech.

Terrorism and internet shutdowns

General Comment No. 34 on the ICCPR states that the media plays an important role in informing the public about acts of terrorism, and it should be able to perform its legitimate functions and duties without hindrance.[374] While some governments argue that internet shutdowns are necessary to ban the spread of news about terrorist attacks to prevent panic or copycat attacks, the UNSR on freedom of expression has instead found that maintaining connectivity may mitigate public safety concerns and help restore public order.[375] Indeed, in their 2011 Joint Declaration on Freedom of Expression and the Internet[376], the freedom of expression mandate-holders stated:

> Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or

[373] UN Special Rapporteur on the promotion and protection of human rights while countering terrorism, 'Statement by the Special Rapporteur on the promotion and protection of human rights while countering terrorism at the International Seminar Terrorism and human rights standards: Santiago de Chile, Chile' (2011) (accessible at: https://newsarchive.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=11737&LangID=E).
[374] UN Human Rights Council, 'General Comment no. 34 at para 46 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[375] UN Human Rights Council, '2017 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' at para. 14 (2017) (accessible at: https://www.undocs.org/A/HRC/35/22).
[376] (2011) (accessible at: https://www.osce.org/files/f/documents/e/9/78309.pdf).

national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet.[377]

PRESCRIBED BY LAW

If national security is to be used to limit freedom of expression, the restriction must not only address a legitimate national security interest but must also be prescribed by law. The exact meaning of this has been an issue in several national security-related cases.

In *Shreya Singhal v. Union of India*,[378] the Supreme Court of India considered a constitutional challenge against section 66A of the Information Technology Act of 2000 by two women who had been arrested and charged under that section for Facebook comments in which they criticised the closure of Mumbai for a general strike (*bandh*) following the death of a political leader. Section 66A prohibited *inter alia* sending via a computer or other communications device information that is 'grossly offensive' or 'menacing', as well "information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device". The Court found the law to be overbroad and too vague to pass constitutional muster, reasoning as follows:

> In point of fact, Section 66A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the Section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total.[379]

The Court found that the law was inconsistent with freedom of expression as guaranteed under Article 19 of the Indian Constitution and invalidated Section 66A in its entirety.[380]

The analysis of the Supreme Court in this case was similar to the analysis under international human rights law of whether a restriction on freedom of expression meets the tripartite test contained in Article 19(3) of the ICCPR. In cases of vague and overbroad provisions, as in *Shreya Singhal v. Union of India*, restrictions would fail to meet the requirement of being provided by law. The UN Human Rights Committee has found that:

> For the purposes of paragraph 3, a norm, to be characterized as a "law", must 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. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.[381]

---

[377] Adopted 1 June 2011.
[378] Writ Petition (Criminal) No.167 of 2012 (2015) (accessible at: https://indiankanoon.org/doc/110813550/).
[379] *Id.* at para. 83.
[380] *Id.* at paras. 98 and 119.
[381] UN Human Rights Comittee, 'General Comment no. 34', UN Doc CCPR/C/GC/34 (2011) at para. 25 (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).

Overbroad restrictions on national security grounds will likely also fail the requirement of proportionality, which is part of the requirement that restrictions be 'necessary' to protect a legitimate interest, such as national security.[382]

NECESSARY IN A DEMOCRATIC SOCIETY

Most cases involving national security restrictions tend to be decided based on necessity or proportionality. One area where restrictions may be deemed unjustifiable is if they are overbroad. Various courts have found that the burden is on the government to show that a restriction on freedom of expression is necessary and proportionate. Courts have also insisted that there must be a close nexus between the restricted expression and an actual risk of harm to national security or public order.

In *Tholal and Mahmood v. Maldives*,[383] the UN Human Rights Committee (UNHRCtte) considered an individual complaint from two citizens of the Maldives. The authors of the complaint were two of the commissioners on the Maldives Human Rights Commission, which had drafted a report on the human rights situation in the Maldives for consideration during the UN Human Rights Council's Universal Periodic Review of the Maldives.[384] The report that had, among other things, called into question the "independence, transparency, impartiality, competence, consistency and accessibility" of the Maldives' judiciary and suggested that the Supreme Court had weakened the powers of lower courts and exercised control over the judiciary.[385] Following the publication of the report, the Supreme Court of the Maldives initiated *suo moto* proceedings against the authors, alleging 20 unlawful acts, including acts against national security.[386] Ultimately, the Court ruled that the authors had violated the Constitution and Judicature Act after finding that they had "deliberately attempted to undermine the independence of the judiciary and the Constitution of the Maldives, and had encouraged acts that damage the Maldives' independence, sovereignty, constitutional system, peace and order."[387] The Court ordered the Commission to follow an 11-point set of guidelines in future operations.[388]

In considering the complaint, the UNHRCtte did not evaluate the truthfulness of the allegations in the Commission's human rights report. The UNHRCtte reasoned that, even if one were to assume the Supreme Court's allegations against the authors and order imposing guidelines for the Commission's future actions were provided by law and pursued a legitimate purpose, they nonetheless failed to meet the requirement of proportionality which was required for any restriction on freedom of expression.[389] In the proportionality analysis, the Committee relied on several factors, including the wide-ranging nature of the allegations and the impact they would have on the ability of the Commission to fulfil its mandate of raising human rights concerns, holding that the restriction

[382] *Id.* at para 34.
[383] Communication No. 3248/2018, UN Doc CCPR/C/130/D/3248/2018 (2021) (accessible : https://ccprcentre.org/files/decisions/G2106296_(1).docx).
[384] *Id.* at para 2.2.
[385] *Id.* at para. 2.3.
[386] *Id.* at paras. 2.4 and 8.3.
[387] *Id.* at para. 2.8.
[388] *Id.* at para 2.9.
[389] *Id.* at paras. 8.4-8.10.

did "not represent the least-intrusive instrument among those which might achieve their function of protecting peace and security".[390]

One challenge with national security restrictions is that they are often worded so broadly that they can be used to target legitimate criticisms of the government. The foundational importance of freedom of expression for democratic governance and accountability and perils of constraining political discourse were articulated by the Sri Lanka Supreme Court in the 1992 case *Perera v. The Attorney-General and Others*:

> Freedom of speech and expression means the right to express one's convictions and opinions freely by word of mouth, writing, printing, pictures or any other mode. It includes the expression of one's ideas through banners, posters, signs etc. It includes the freedom of discussion and dissemination of knowledge. It includes freedom of the press and propagation of ideas, this freedom is ensured by the freedom of circulation. The right of the people to hear is within the concept of freedom of speech. There must be untramelled [*sic*] publication of news and views and of the opinions of political parties which are critical of the actions of the government and expose its weaknesses. Debate on public issues should be uninhibited, robust and widely open and that may well include vehement, caustic and sometimes sharp attacks on government.[391]

PRIOR RESTRAINT IN NATIONAL SECURITY CASES

There is a general presumption in international law against prior restraint of freedom of expression on the basis that it is unnecessary and disproportionate, and has a chilling effect on the enjoyment of this right. The European Court of Human Rights has found that the "dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court", especially when applied to the press in view of the 'perishable' nature of news, which loses value when delayed.[392]

Principle 23 of the Johannesburg Principles provides: "Expression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country."[393] This recognises that in cases of national security there may sometimes, exceptionally, be a need to prevent the dissemination of information prior to publication, but only in the very most serious public emergencies.

This was also the question that the United States Supreme Court confronted in *New York Times Co. v United States*,[394] better known as the "Pentagon Papers" case. The government sought prior restraint on publication of a large number of documents — 47 volumes of them — labelled "top secret" and leaked from the Department of Defense.

---

[390] *Id.* at para. 8.9.
[391] 1992 1 Sri L.R. (1992) at p. 202 (accessible at: https://www.lawnet.gov.lk/joseph-perera-alias-bruten-perera-v-the-attorney-general-and-others/).
[392] *Observer and Guardian v. United Kingdom*, Application No. 13585/88 (1991) at para. 60 (accessible at: http://hudoc.echr.coe.int/eng?i=001-57705).
[393] Johannesburg Principles, above at n. 11.
[394] United States Supreme Court, Case 403 US 713 (1971) (accessible at: https://www.law.cornell.edu/supremecourt/text/403/713).

The documents detailed the decision-making leading to the United States' involvement in the Vietnam war and the government sought to prevent publication because of alleged damage to national security and relations with other countries.

In a brief judgment rejecting the request for prior restraint, the Court drew on earlier judgments to note that prior restraint can only be allowed in extreme circumstances:

> "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity" … The Government "thus carries a heavy burden of showing justification for the imposition of such a restraint."[395]

Individual opinions by the judges elaborated on this reasoning. For example, Justice Hugo Black argued:

> "The word "security" is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security..."[396]

National security is also frequently relied upon as a reason for justifying an interference with access to the internet, which is another form of prior restraint. While this may, in appropriate circumstances, be legitimate, it also has the potential to be relied upon to quell dissent and cover up state abuses and is always disproportionate when applied to an entire geographic area through an internet shutdown. (For more on this, see Module 3 of this series on access to the internet.)

The covert nature of many national security laws, policies and practices, as well as the refusal by states to disclose complete information about threats to national security, tends to exacerbate this concern.

CONCLUSION

National security remains a common justification offered by states for limiting freedom of expression by journalists, bloggers, and media organs. However, it is often used not to protect security but to quell dissent and cover up state abuses. Increasingly, courts are limiting the scope of application of national security laws as they are often vague and drafted with a view to circumventing constitutional checks and balances. Activists, lawyers, and members of the media should, however, remain vigilant and test all national security-related laws for compliance with international law, including the Johannesburg, Tshwane and Siracusa Principles.

[395] *Id.*
[396] *Id.*

MODULE 10: VIOLENCE AGAINST JOURNALISTS

- **Violence against journalists, especially in retaliation for their work, poses a serious threat to freedom of expression, whether it takes the form of physical or online attacks.**
- **States, in addition to avoiding ensuring that State actors do not engage in attacks, have a responsibility to take due diligence to prevent violence, protect journalists and investigate, prosecute and redress any attacks that are perpetrated.**
- **Protection of confidential journalistic sources is also important to protecting journalists and ensuring freedom of expression more generally.**
- **States must incorporate gender-sensitive approaches when responding to violence against journalists, given the prevalence of gender-based violence against female journalists.**
- **Practical steps may include developing a national plan of action or a specialised safety mechanism to address violence against journalists.**

INTRODUCTION

Violence against journalists and others for exercising their right to freedom of expression poses a particularly serious threat to the realisation of this right. Besides violating the rights of the targets, such violence may lead to journalists self-censoring, especially by avoiding reporting on important but sensitive topics such as corruption, organised crime or human rights violations. This in turn harms the rights of society as a whole to access information about these issues freely.

This Module provides an overview of State obligations under international human rights law to address violence against journalists. It first gives a brief overview of the scope of State obligations to create a favourable environment for freedom of expression. It then looks specifically at State obligations to respond to physical and online violence against journalists, protection of journalistic sources, and gender-based violence. It ends with a discussion of practical approaches to combatting violence.

THE DUTY TO PROVIDE A FAVOURABLE ENVIRONMENT FOR FREEDOM OF EXPRESSION

States have a duty to promote a favourable environment for freedom of expression. On the one hand, this means avoiding taking actions which harm or interfere with the exercise of the right ("negative obligations"). On the other, it also encompasses positive obligations to promote and protect freedom of expression.

International human rights treaties generally impose obligations on State Parties to adopt laws or other measures necessary to give effect to the rights in the Covenant. These may

include "legislative, judicial, administrative, educative and other appropriate measures".[397] States also have certain obligations to protect people from acts by private parties which harm their enjoyment of human rights. States are not fully responsible for the acts of third parties, but they must not fail to respond appropriately in the face of rights violations, including to "exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities."[398]

In the context of the right to freedom of expression, creating an enabling environment for freedom of expression requires States to take a range of actions, such as promoting media diversity and guaranteeing access to information. In addition, States should take steps to ensure that those who exercise their right to freedom of expression are not subject to retaliation for doing so, including violent attacks or other threats.[399]

PHYSICAL ATTACKS

> *"The most extreme form of censorship is to kill a journalist. The killing not only silences the voice of the particular journalist, but also intimidates other journalists and the public in general." – UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns*[400]

UNESCO's *Observatory on Killed Journalists* documents 1529 journalists and media workers who have been killed since 1993.[401] Impunity for these cases is unfortunately high: as of 2020, only 13% of the cases had been resolved.[402] A number of countries in South and Southeast Asia are among the worst performers, including the Philippines (112), Pakistan (86), Afghanistan (81), India (65), Bangladesh (25) and Sri Lanka (12).[403] The Committee for the Protection of Journalists also includes Afghanistan, the Philippines,

---

[397] Human Rights Committee, 'General Comment No. 31' (2004), para. 7.
[398] *Id.* at para. 8.
[399] See, for example, Council of Europe, 'Recommendation CM/Rec(2016)4 of the Committee of Ministers to Member States on the protection of journalism and safety of journalists and other media actors' (2016) at paras. 13, 15 (accessible at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415d9).
[400] Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, A/HRC/20/22 (2012) at para. 21.
[401] The data tracks killings of "journalists, media workers and social media producers who are engaged in journalistic activity". UNESCO Director-General's Report on the Safety of Journalists and the Danger of Impunity, https://en.unesco.org/themes/safety-journalists/dgreport/methodology. The Committee to Protect Journalists, with a slightly different methodology, counts 1449 journalists or 1565 journalists and media workers killed with a confirmed motive in a similar time period (1992-2022), https://cpj.org/data/killed/?status=Killed&motiveConfirmed%5B%5D=Confirmed&type%5B%5D=Journalist&start_year=1992&end_year=2022&group_by=year.
[402] IPDC, 'Direct-General Report on the Safety of Journalists and the Danger of Impunity' (2020) at p. 18 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000374700/PDF/374700eng.pdf.multi).
[403] UNESCO, 'Observatory of Killed Journalists', https://en.unesco.org/themes/safety-journalists/observatory.

Pakistan, Bangladesh and India on its impunity index, which counts countries with more than five unsolved journalist murders.[404]

While killings are a particularly grave example of violence against journalists, other forms of violence also have serious impacts on the realisation of freedom of expression. These include, for example, torture, arbitrary arrest or detention, enforced disappearances, intimidation or harassment, and threats. Data on such acts is more challenging to track, but they can have serious consequences for freedom of expression.

None of these kinds of attacks on journalists, if based on their exercise of freedom of expression, can be justified "under any circumstance".[405] Such acts not only violate freedom of expression but also may violate other fundamental human rights, such as the right to life, the right to be free from torture, the right to liberty and security of the person, or the right to be free from interference with one's privacy, family or home life.

States must first ensure that their own agents do not commit violence against journalists. State officials must, in addition to avoiding acts of violence themselves, "control and adequately supervise their officers". [406] On the other hand, lower-level officials should not be able to rely on a defence of obedience to superior orders for these kinds of serious crimes.[407] Government officials should also take care to avoid making public statements which stigmatise the media, threaten journalists or undermine respect for media independence. [408]

States also have positive obligations to create a safe environment for journalists. This means exercising due diligence to address attacks on journalists by non-State actors. A State's positive obligations in these areas can be summarised as an obligation to prevent, to protect and to investigate, prosecute and redress.

- **Preventing violence against journalists**: States should take action to prevent violence against journalists, including "prevention mechanisms and actions to address some of the root causes of violence against journalists and of impunity."[409] These preventative measures

[404] Jennifer Dunham, 'Killers of Journalists Still Get Away with Murder, Committee to Protect Journalists', (2021) (accessible at: https://cpj.org/reports/2021/10/killers-of-journalists-still-get-away-with-murder/#index).
[405] Human Rights Committee, 'General Comment No. 34' at para. 34.
[406] Investigation of, accountability for and prevention of intentional State killings of human rights defenders, journalists and prominent dissidents: Report of the Special Rapporteur on extra judicial, summary or arbitrary executions, A/HRC/41/36 (2019) at para. 29.
[407] Human Rights Committee, 'General Comment No. 31' at para. 18.
[408] International Mechanisms for Promoting Freedom of Expression, '2018 Joint Declaration on Media Independence and Diversity in the Digital Age', para. 4(b), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1100&lID=1; Investigation of, accountability for and prevention of intentional State killings of human rights defenders, journalists and prominent dissidents: Report of the Special Rapporteur on extra judicial, summary or arbitrary executions, A/HRC/41/36 (2019) at para. 29.
[409] UN Plan of Action on the Safety of Journalists and the Issue of Impunity, CI-12/CONF.202/6 at para. 1.6 (accessible at: https://en.unesco.org/sites/default/files/un-plan-on-safety-journalists_en.pdf).

may include amending legal frameworks to criminalise properly acts of violence against journalists, revising the media law framework to enable the media to engage freely in journalistic activity without interference, undertaking awareness-raising and education efforts, monitoring and reporting on attacks on journalists, or training security personnel, among others.[410]

Compelling Good Behaviour from Investigatory Authorities: A Case from Pakistan

While investigatory authorities have primary responsibility for taking measures to prevent their own agents from harassing or using violence against journalists, courts can also order or recommend institutional changes. A good example is the decision of the Islamabad High Court in *Rana Muhammad Arshad v. Pakistan*. The journalist in this case had received a vague notice issued by the Federal Investigating Agency under the Prevention of Electronic Crimes Act, followed by a raid of his residence, apparently because of a tweet he had disseminated.

The Court noted an increase in complaints about vague notices under the Prevention of Electronic Crimes Act. It expressed concern that this was either the result of a misinterpretation of the law or an attempt to suppress journalism, contrary to the duty of the State to avoid any actual or perception of an abuse of its powers in order to threaten the press.[411] The Court instructed the Federal Investigating Agency to formulate guidelines for investigating officers and to consider prescribing special guidelines regarding investigations of journalists, in light of the importance of freedom of the press. The Court also suggested that the government should consider establishing a mechanism for handling complaints about violations of freedom of the press and hold consultations with press institutions to understand their perceptions about media intimidation by authorities.[412]

- **Protecting at-risk journalists:** States should also adopt "effective measures" to protect journalists from attacks.[413] They could include issuing protective orders promptly, establishing specific information-gathering mechanisms or creating early warning mechanisms.[414] It could also include offering specific protection to at-risk journalists, such as safety equipment, hotlines or even guards where needed.

[410] International Mechanisms for Promoting Freedom of Expression, '2012 Joint Declaration on Crimes against Freedom of Expression' (accessible at: https://www.osce.org/representative-on-freedom-of-media/91595); Human Rights Council, 'Resolution 21/12', A/HRC/RES/21/12 (2012) at para. 8.
[411] *Rana Muhammad Arshad v. Pakistan*, Islamabad High Court, W.P. No. 2939/2020 (2020), para. 10 (accessible at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2022/05/W.P-2939-2020_637406912282280654.pdf).
[412] *Id.* at para. 11.
[413] Human Rights Committee, 'General Comment No. 34', para. 23.
[414] Human Rights Council Resolution 33/2, A/HRC/RES/33/2 (2016), para. 6.

In some cases, particularly in countries with recurring incidents of violence against journalists, specialised protection mechanisms should be created. Such mechanisms may incorporate features such as an urgent action procedure where journalists can request protective support.

When a State fails to take steps to protect a specific journalist who is at risk, that State may violate its obligation to protect. Whether the State has taken sufficient steps to protect a journalist will depend on the facts. However, in assessing State obligations in these cases, the European and Inter-American regional human rights courts have relied upon the following standard: whether authorities knew or should have known of a real and immediate danger to the journalist and failed to take reasonable protective measures.[415]

- **Investigation, prosecution and redress of attacks**: When an attack on a journalist occurs, authorities have a responsibility to take effective steps to investigate and prosecute that crime, and ensure that proper redress is provided. Failing to do so may violate Article 2(3) of the ICCPR (or the equivalent in other treaties), which requires effective remedies for human rights violations, in addition to freedom of expression and other implicated rights.[416]

  The investigation and prosecution of such crimes should meet certain minimum standards. They should be investigated thoroughly and rigorously, in a timely manner, and by impartial and effective authorities.[417] Ensuring these standards are met will require certain institutional efforts, such as ensuring investigatory units are sufficiently well-resourced and that the independence of courts is protected.[418]

  In examining individual cases, human rights courts have looked at a variety of factors when assessing whether the State has fulfilled its obligations. Examples where this obligation was not met include:

[415] See, for example, Inter-American Court of Human Rights, *Pueblo Bello Massacre v. Colombia* (2006), Series C, No. 140 at para. 123 (available at: http://www.corteidh.or.cr/docs/casos/articulos/seriec_140_ing.pdf); and European Court of Human Rights, *Osman v. United Kingdom* (1998), Application No. 23452/94 at para. 116 (available at: http://hudoc.echr.coe.int/eng?i=001-58257). Although *Osman* itself did not specifically address freedom of expression, elsewhere the Court has found violations of freedom of expression (along with other rights) for failures to protect journalists from attack. See *Dink v. Turkey* (2010), Application Nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09 (available at: https://hudoc.echr.coe.int/eng-press?i=003-3262169-3640194); and *Özgür Gündem v. Turkey* (2000), Application No. 23144/93 (available at: https://hudoc.echr.coe.int/eng-press?i=003-68306-68774).

[416] Human Rights Committee, 'General Comment No. 31' at para. 18. See also Human Rights Committee, *Jit Man Banet and Top Bahadur Basnet v. Nepal*, Communication No. 201/2011, para. 8.8 (accessible at: https://juris.ohchr.org/Search/Details/1904).

[417] Human Rights Council, 'Resolution 27/5', A/HRC/RES/27/5, 2 October 2014 at para. 2-3; and International Mechanisms for Promoting Freedom of Expression, '2012 Joint Declaration on Crimes against Freedom of Expression' at para. 4.

[418] International Mechanisms for Promoting Freedom of Expression, '2012 Joint Declaration on Crimes against Freedom of Expression'.

- Unjustified or unreasonable delays in investigation and prosecution, such as when Russia failed to provide "convincing and plausible" reasons for lengthiness of investigations into the assassination of a journalist.[419]
- Insufficient independence for responsible government authorities, such as when a Colombian military tribunal investigated alleged attacks on a journalist by members of the military.[420]
- Failing to investigate whether a journalist's murder was linked to his work as a journalist.[421]

Proper redress includes not only obtaining a conviction but also ensuring the victim (or family members) are appropriately compensated. Such reparations may include broader restitution or rehabilitation measures such as public apologies or memorials, guarantees to prevent such crimes in the future or changing laws and practices.[422]

Finally, while this Module deals with human rights law, journalists are also protected under international humanitarian law, which governs armed conflicts. Under international humanitarian law, journalists are considered to be civilians, not combatants.[423] Like other civilians present in a war zone, they should not be the subject of intentional military attacks.

ONLINE VIOLENCE, SUCH AS ABUSE, TROLLING AND SMEAR CAMPAIGNS

Online violence can sometimes be seen as less serious than offline violence. However, online violence and harassment can be linked to offline threats, and may serve as a predictor of a real-world threat or accelerate into offline attacks. In one survey of female journalists, for example, 20% of respondents reported offline attacks or abuse linked to online violence they had experienced.[424] Further, given that most modern communication occurs online, online harassment can have a dramatic impact on the exercise of freedom of expression, especially if the targets of such harassment self-censor in response.

Journalists may now experience forms of violence and harassment that are uniquely enabled by digital communications.[425] Some examples include:

---

[419] European Court of Human Rights, *Mazepa and others v. Russia* (2018), Application No. 15086/07 at para. 80-8 (accessible at: https://hudoc.echr.coe.int/eng?i=001-184660).
[420] *Vélez Restrepo y Familiares v. Colombia* (2012), Series C No. 248, https://corteidh.or.cr/docs/casos/articulos/seriec_248_esp.pdf (only available in Spanish but a summary in English is accessible at: https://www.corteidh.or.cr/docs/casos/articulos/resumen_248_ing.pdf)
[421] European Court of Human Rights, *Adali v Turkey* (2005), Application No. 381187/97 (accessible at: https://hudoc.echr.coe.int/eng?i=001-68670); and *Kilic v. Turkey* (2000), Application No. 22492/93 (accessible at: https://hudoc.echr.coe.int/eng?i=001-164693).
[422] Human Rights Committee, 'General Comment No. 31' at para. 16.
[423] International Committee of the Red Cross, 'Customary IHL Database, Rule 34: Journalists' (accessible at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule34).
[424] Julie Posetti, *et al.*, *Online Violence against Women Journalists*, UNESCO (2020) at p. 3 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000375136/PDF/375136eng.pdf.multi).
[425] Report of the Secretary-General, 'Safety of Journalists and the Issue of Impunity' (2021), A/76/285 at para. 6.

- Doxing, or sharing via the Internet of private identifying information such as name, location and address, can be particularly dangerous for journalists because it may allow would-be attackers to locate and harm them.
- Trolling, or posting or sending insulting or inflammatory messages about a specific person, can be harmful to a journalist's sense of safety and well-being. In the offline context, such harassment would typically be limited in scale but in the digital age trolling can occur at a mass scale or a high rate of frequency, inundating the target with harmful messages.
- Smear campaigns can similarly attempt to damage a journalist's reputation. While not unique to the digital era, such campaigns can again be mobilised on a much larger scale and be conducted more visibly and effectively than offline.
- On social media platforms, bots can mimic human activity, such as posting comments. Bot activity can be used to coordinate smear or trolling campaigns, particularly when well-funded or criminal elements have an interest in promoting a certain message or targeting a particular person.
- Cyberattacks can be directed at journalists or media institutions. Such cyberattacks may aim to insta4ll spyware on a journalist's phone, for example, or take down a news website.

A major concern with these kinds of attacks on journalists is the extent to which they are coordinated or planned by malicious actors with the intent of discrediting or harming the journalist.[426] The origin of such coordinated attacks can be difficult to trace, but they sometimes originate in powerful State or non-State actors who have in interest in silencing a journalist.

As in the offline context, State actors should refrain from engaging in online violence against journalists, either directly or indirectly. For example, public officials should avoid making threats against journalists online. Politicians should ensure that their campaign staff or supporters are not engaged in disinformation-based smear campaigns about journalists.

States positive obligations include taking steps to address online violence by private actors. However, two main caveats arise here. First, State regulation of online content should be in strict compliance with international standards, noting that most of the online attacks described above involve expressive behaviour. As already described in earlier modules, regulation of online content is frequently overbroad or inappropriately tailored to the harm in question. In such cases, laws regulating online speech are often weaponised *against* journalists instead of offering them protection. Second, challenging questions arise around the extent to which State action against online harassment of journalists can be fully effective. The policies of private sector actors, such as large social media companies that operate globally, may have a more direct impact on the experience of journalists.

Notwithstanding these caveats, States can still play a key role in responding to online violence against journalism by private actors. For example:

[426] *Id.* at para. 8.

- States should ensure to create an enabling environment for journalists online, including by eliminating laws which inappropriately criminalise online speech.[427]
- Surveillance regimes and data protection laws should be reviewed to ensure that journalist identity and confidentiality of sources is protected. Targeted surveillance of journalists, in particular, can lead to self-censorship. Surveillance of journalists on account of their legitimate exercise of freedom of expression is never appropriate.[428]
- States should engage in a range of awareness-raising and educational campaigns and initiatives specific to online violence against journalists.
- States should strengthen the ability of law enforcement officials and others to respond properly to online violence, for example by training them properly on how to respond to such attacks or improving their capacity to investigate and prosecute crimes in the digital space.[429]
- States should also take steps to protect journalists against cyberattacks which may put them at risk, such as by taking steps to protect digital communications systems from such attack or supporting cybersecurity measures for at-risk journalists.[430]

In addition, States should adopt "effective laws and measures" to prevent online attacks on journalists, but only where they respect principles related to freedom of expression.[431] This includes principles on intermediary liability and Internet freedom discussed in earlier modules. However, within these bounds, States could explore laws which compel private actors, and particularly social media companies, to take greater responsibility for online violence against journalists occurring on their platforms. Examples could potentially include asking major platforms to monitor and report on violence against journalists or imposing transparency requirements regarding measures taken in response to online violence. The question of regulating major social media platforms is a complex and rapidly evolving one, however, and better practices in the specific area of journalist safety have yet to emerge.

PROTECTION OF JOURNALISTIC SOURCES

Protection of confidential journalistic sources is a core component of media ethics. Normally, journalists openly identify their sources but, if doing so would breach a promise made to the source, journalists will protect the source's confidentiality. The ability of a journalist to protect confidential sources protects the willingness of sources to share information with journalists in the first place, and thereby protects the rights of society as a whole to access information about sensitive issues. Accordingly, the Human Rights Committee has said: "States parties should recognise and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not o disclose information sources."[432] Maintaining

[427] *Id.* at para. 14.
[428] Report of the Special Rapporteur on freedom of expression, 'Surveillance and human rights' (2019), A/HRC/41/35, para. 26.
[429] Report of the Secretary-General, 'Safety of Journalists and the Issue of Impunity' (2021), A/76/285 at para. 59.
[430] International Mechanisms for Promoting Freedom of Expression, '2012 Joint Declaration on Crimes against Freedom of Expression'.
[431] Report of the Secretary-General, 'Safety of Journalists and the Issue of Impunity' (2021), A/76/285 at para. 57.
[432] Human Rights Committee, 'General Comment No. 34' at para. 45.

confidentiality may also be crucial to journalists' own safety; journalists may be targeted if they are seen as potential witnesses rather than independent or confidential observers, for example.[433]

Traditionally, concerns over protecting journalistic sources primarily arose in the context of court proceedings when courts sought to compel journalists to reveal their confidential sources. Clear rules should be set out in law which only allow source disclosure to be ordered in exceptional circumstances. For example, in a landmark European Court of Human Rights Case, *Goodwin v. United Kingdom*, the Court affirmed that journalists should only be compelled to reveal a source in "exceptional circumstances where vital public or individual interests were at stake".[434] Protecting journalistic sources is "one of the basic conditions for press freedom", so in order to meet the requirement of necessity under the three-part test, there must be an "overriding requirement in the public interest" justifying disclosure. [435]

Protection of Journalistic Sources in the Asia Region

In Malaysia, in 2013, a major High Court ruling affirmed the importance journalistic protection of confidential sources. In *Datuk Seri Tiong King Sing v. Datuk Seri Ong Tee Keat*, the Court considered first whether the disclosure of sources was relevant and necessary, and found that in the case it was. However, because the harm caused by requiring disclosure would outweigh the benefits, the Court decided it was in the public interest to decline to mandate disclosure.[436]

Similarly, Singapore's Court of Appeals, in *Dorsey James Michael v. World Sport Group Pte Ltd*, considered whether to allow an interrogation in a civil suit which would have compelled a journalist who blogged about a football corruption scandal to reveal his sources. The Court emphasised that "necessity" is "the main cornerstone" in such cases; the party requesting the interrogation must show that they need to identify the sources for the viability of their case, rather than that they are merely on a fishing expedition.[437] Where revealing sources is involved, the Court noted that the party trying to learn the

[433] International Criminal Tribunal for the former Yugoslavia, *Prosecutor v. Radoslav Brdjanin Momir Talic,* Decision on Interlocutory Appeal, Case No. IT-99-36-AR73.9, 11 December 2022, para. 42-43; IACHR, Office of the Special Rapporteur for Freedom of Expression, 'Violence against journalists and media workers' (2013) at p. 36 (accessible at: https://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_Violence_WEB.pdf).
[434] *Goodwin v. United Kingdom* (1996), Application No. 17488/90, Grand Chamber at para. 37 (accessible at: https://hudoc.echr.coe.int/eng?i=001-57974).
[435] *Id.* at para. 39.
[436] High Court Malaya, Kuala Lumpur, *Datuk Seri Tiong King Sing v. Datuk Seri Ong Tee Keat* (2013), Suit No. S-23-99-2009, (accessible at: http://www.cljlaw.com/default.asp?page=cotw140523&scrollto=COTW3).
[437] Singapore Court of Appeal, *Dorsey James Michael v. World Sport Group Pte* (2014), 2014 SGCA 4 at para. 47 (accessible at: https://web.archive.org/web/20150722041319/http:/www.singaporelaw.sg/sglaw/laws-of-singapore/case-law/free-law/court-of-appeal-judgments/15485-dorsey-james-michael-v-world-sport-group-pte-ltd-2014-sgca-4).

source identity must show a "real interest" in suing the source whose identity is requested. Such an interest must be weighed against the public interest in retaining confidentiality. In balancing the "real interest" against the "public interest", reference should be had to factors such as whether granting disclosure would be a "necessary and proportionate response", how confidential the information was, and whether the information could be obtained from another source.[438]

In this case, World Sport Group had not demonstrated that it was necessary for them to obtain the identity of the sources. Further, the Court gave an extended discussion of the public interest in combatting corruption, suggesting that where there is high public interest in the information disclosed by confidential sources, such as in accountability for corruption, source confidentiality should be maintained.[439]

Outside the context of court proceedings, source confidentiality concerns also arise during searches and seizures of journalists' homes, workplaces and property. The importance of protecting source confidentiality imposes a higher burden on police or investigatory authorities when they search media premises or journalist residences.[440] The European Court of Human Rights, for example, has said that prior to seizure of journalistic material or raids of media premises, a judge or independent body must evaluate the risk to source confidentiality against the public interest in the investigation, and consider whether a less intrusive search could meet the investigatory needs.[441]

However, in the modern era, digital communications have dramatically changed the manner in which both State and non-state actors can attempt to access confidential journalistic material or sources. Expanded legal grounds for surveillance combined with the technical tools to do so may create a "work around" for journalistic privilege, enabling governments to access sources outside of a court process and without the knowledge of journalists.[442]

International human rights standards clearly condemn such practices. As stated in the Declaration of Principles on Freedom of Expression and Access to Information in Africa, for example, "States shall not circumvent the protection of confidential sources of information or journalistic material through the conduct of communication surveillance except where

[438] *Id.* at paras. 47-48.
[439] *Id.* at paras. 71-79.
[440] Report of the Special Rapporteur on freedom of expression, A/70/361 (2015) at para. 24 (giving examples of laws which limit search and seizure of journalistic material).
[441] *Sanoma Uitgevers B.V. v. The Netherlands* (2014), Grand Chamber, Application No. 38224/03 at paras. 89-92 (accessible at: https://hudoc.echr.coe.int/eng?i=001-100448).
[442] For an in-depth discussion of this issue, see Julie Posetti, *Protecting Journalism Sources in the Digital Age*, UNESCO (2017) (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000248054) (including an overview of the Asia and Pacific region beginning at p. 67).

such surveillance is ordered by an impartial and independent court and is subject to appropriate safeguards."[443]

Similarly, in their 2018 Joint Declaration, the special international mandates on freedom of expression noted: "States should put in place effective practical and enforceable measures to avoid identifying confidential journalistic sources indirectly using digital means and should avoid taking actions that result in media outlets or journalists being used as an indirect means to pursue criminal investigations."[444]

The European Court of Human Rights, in *Big Brother Watch v UK*, found that a surveillance scheme violated the right to freedom of expression where it did not offer sufficient protection for journalistic source confidentiality. United Kingdom law had safeguards for source confidentiality when authorities specifically sought authorization to obtain data identifying a specific source. However, the broader bulk surveillance regime, including general requests for journalist communications data, did not incorporate any such safeguards.[445] This meant, for example, that analysts could target journalists' communications for examination without any judicial order or application of the criteria set out in *Goodwin*, discussed above. [446]

Another key impact of the digital era is the changing nature of media work. A wide range of actors now engage in journalistic-type activities. For this reason, many international standards discussing source confidentiality apply the journalistic privilege broadly, such as to any "social communicator"[447] or "person regularly engaged in the collection and dissemination of information to the public".[448] National legal systems are increasingly adapting to recognise this reality. For example, it is noteworthy that in the Singapore *Dorsey* case described above, the journalist in question was a blogger, not a formal journalist in the traditional sense.

GENDER-BASED VIOLENCE

The Committee on the Elimination of Discrimination against Women defines gender-based violence to include that "which is directed against a woman because she is a woman

[443] African Commission on Human and Peoples' Rights, adopted at 65th Ordinary Session, 21 October – 10 November 2019, Principle 25(3) (accessible at: https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf).
[444] International Mechanisms for Promoting Freedom of Expression, '2018 Joint Declaration on Media Independence and Diversity in the Digital Age'.
[445] *Big Brother Watch and others v United Kingdom* (2021), Application Nos. 58170/13, 62322/14 and 24960/15 at paras. 524-525 (accessible at: https://hudoc.echr.coe.int/eng?i=001-210077).
[446] *Id.* at paras. 444-445, 457.
[447] Inter-American Commission on Human Rights, The Inter-American Declaration of Principles on Freedom of Expression, adopted at 108th session, 2-20 October 2000.
[448] Council of Europe, 'Recommendation No. R (2000) 7 of the Committee of Ministers to Member States on the right of journalists not to disclose their sources of information' (2000).

or that affects women disproportionately".[449] States have an obligation to avoid perpetrating such violence themselves, but must also take "all appropriate measures to prevent, as well as to investigate, prosecute, punish and provide reparations for, acts or omissions by non-State actors that result in gender-based violence against women".[450] Violence against female journalists on account of their work is, like all such forms of violence, an attack on freedom of expression.

Accordingly, States are obliged to address violence against female journalists not only under their obligations to protect freedom of expression but also as part of their obligations to address discrimination against women. United Nations bodies, including the Human Rights Council, Security Council and the General Assembly, have issued resolutions strongly condemning attacks on female journalists.[451] For example, the Human Rights Council:

> "*[C]ondemns unequivocally* the specific attacks on women journalists and media workers in relation to their work, such as gender-based discrimination, including sexual and gender-based violence, threats, intimidation and harassment, online and offline"[452]

In practice, however, female journalists continue to experience gender-based violence in the course of their work. Women represent a small portion of the journalists who are killed while pursuing journalistic work. However, female journalists are disproportionally likely to experience gender-based violence.[453] Sexual violence, sexual harassment, online harassment, rape and the threat of rape are all tools used to intimidate female journalists and discourage their work. Such acts are underreported, due to cultural stigmas or fear of retaliation in the workplace.[454] Other types of sexist harassment or threats can also have serious consequences. One global survey of female journalists found that 37% avoided reporting on certain topics because of attacks or harassment they had experienced.[455]

Female journalists are also much more likely to experience certain forms of online violence.[456] A major 2020 UNESCO report on the topic found that 73% of female journalists who responded had experienced online violence. 42% were targeted with reputational threats, 25% received threats of physical violence, 18% were threatened with sexual

---

[449] Committee on the Elimination of Discrimination against Women, 'General Recommendation No. 35 on gender-based violence against women' (2017), CEDAW/C/GC/35, para. 1.
[450] *Id.* at para. 24.
[451] For a comprehensive list, see https://en.unesco.org/themes/safety-journalists/women-journalists/UN-resolutions-and-reports.
[452] Human Rights Council, 'Resolution 45/18' (2020), A/HRC/RES/45/18 at para. 2.
[453] Report of the Special Rapporteur on violence against women, 'Combating violence against women journalists' (2020), A/HRC/44/52 at para. 17.
[454] *Id.* at paras. 23-31.
[455] Michelle Ferrier, *Attacks and Harassment: The Impact on Female Journalists and Their Reporting*, International Women's Media Foundation and Trollbusters (2018), p. 44 (accessible at: https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf).
[456] Report of the Special Rapporteur on freedom of expression (2021), A/76/258 at para. 45.

violence, and 13% received threats directed at persons close to them.[457] For 12% of respondents, the effects of online violence were so serious that they sought medical or psychological help.[458] Some forms of online attacks are particularly gendered, such as the non-consensual sharing of intimate images, harassment via misogynistic or sexualised content, or the use of "deepfake" videos (videos which appear to portray someone but in fact are fake and yet this is very to detect) to harm the reputation of female journalists.[459]

Given the distinctive harms experienced by female journalists, as well as cultural and social factors which may impact their experience of violence, measures taken to address journalist safety must take a gender sensitive approach.[460] For example:

- **Preventative measures** should specifically address gender-based violence. This could include initiatives to combat harmful gender-based stereotypes, incorporate gender-sensitive content into awareness-raising and training programmes about violence against journalists, collect sex-disaggregated data about attacks on journalists or develop gender-sensitive investigation procedures.[461] Public officials and authorities are also encouraged to avoid misogynist or discriminatory language towards female journalists.[462]
- **Protection mechanisms** should also be gender-sensitive. Plans and protocols designed for the protection of journalists, for example, should address gender-specific risks and needs.[463]
- **Investigation, prosecution and redress** should also incorporate gender considerations. Violence against women is often under-reported due to fear of further retaliatory attacks and cultural stigmas, especially around sexual violence. Gender-sensitive training of investigatory and prosecutorial authorities is therefore particularly important. States may also specifically need to strengthen their ability to investigate and respond to online gender-based violence.

In the online context, many of the major platforms have introduced initiatives to address women's safety but smaller or newer platforms may still lack such initiatives.[464] Further, many women report that complaints about gender-based violence on online platforms are not adequately addressed and that there is limited transparency around how complaints are

---

[457] Julie Posetti, *Protecting Journalism Sources in the Digital Age*, UNESCO (2017), p. 5 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000248054).
[458] *Id* at p. 6.
[459] Report of the Secretary-General, 'Safety of Journalists and the Issue of Impunity' (2021), A/76/285, para. 9; and Report of the Special Rapporteur on violence against women, 'Combating violence against women journalists', 6 May 2020, A/HRC/44/52 at paras. 41-42
[460] Report of the Special Rapporteur on freedom of expression, A/HRC/20/17 (2012) at para. 52.
[461] United Nations General Assembly, 'Resolution 74/157 on the safety of journalists and the issue of impunity' (2020), A/RES/74/157 at para. 11; and Committee on the Elimination of Discrimination against Women, 'General Recommendation No. 35 on gender-based violence against women' (2017), CEDAW/C/GC/35 at para. 30.
[462] Human Rights Council, 'Resolution 45/18' (2020), A/HRC/RES/45/18 at para. 7.
[463] IACHR, Office of the Special Rapporteur for Freedom of Expression, *Violence against journalists and media workers* (2013) (accessible at: https://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_Violence_WEB.pdf).
[464] Report of the Secretary-General, 'Safety of Journalists and the Issue of Impunity' (2021), A/76/285 at paras. 79, 80.

handled.[465] Greater efforts are needed to protect women from gender-based violence online, but platforms need to develop such policies transparently, in consultation with civil society and leading experts, and in a manner which reflects concern for principles of freedom of expression.

While this discussion has focused on gender-based violence against women, gender non-conforming journalists may experience particularly harmful forms of gender-based violence which also require correspondingly gender-sensitive responses.

PRACTICAL APPROACHES

Violence against journalists can arise from a complex mix of factors, such as a culture of impunity for such crimes, a climate of insecurity in a country, insufficient respect for the independence of the press or an ongoing violent conflict. Responding effectively to violence against journalists therefore requires a comprehensive, tailored State response. Countries with lower levels of violence against journalists should undertake some initiatives, such as monitoring attacks. However, countries with high levels of violence should consider a comprehensive plan or response, including developing a national specialised safety mechanism.

National specialised safety mechanisms are protection initiatives specifically designed normally to enhance protection of journalists or the effectiveness of investigation or protection systems. The most well-known example of such a mechanism is Colombia's protection programme, which establishes a National Unit for Protection and offers physical protection for threatened journalists, potentially even including bodyguards and armoured cars.[466] While these kind of physical protection actions are often important, strong national safety mechanisms should ideally be comprehensive and consider a range of preventative, protective and investigative measures. For guidance on establishing a safety mechanism, see Supporting Freedom of Expression: A Practical Guide to Developing Specialised Safety Mechanisms.[467]

At the international level, the United Nations has developed a Plan of Action on the Safety of Journalists and the Issue of Impunity.[468] The Plan of Action includes five core proposed actions for the UN: 1) strengthening UN mechanisms; 2) cooperating with Member States; 3) partnering with other organisations and institutions; 4) raising awareness; and 5)

[465] Inter-American Commission of Human Rights, Office of the Special Rapporteur for Freedom of Expression, 'Women Journalists and Freedom of Expression' (2018) at para. 9, (accessible at: http://www.oas.org/en/iachr/expression/docs/reports/WomenJournalists.pdf).
[466] For a discussion of this mechanism, see IMS, *Defending Journalism* (2017) (accessible at: https://www.mediasupport.org/publication/defending-journalism/?preview=true).
[467] Toby Mendel, 'Supporting Freedom of Expression: A Practical Guide to Developing Specialised Safety Mechanisms', UNESCO and CLD (2016) (accessible at: http://www.law-democracy.org/live/wp-content/uploads/2016/04/Safety-Report.16.04.20_final.pdf).
[468] UNESCO and IPDC, UN Plan of Action on the Safety of Journalists and the Issue of Impunity (2012), CI-12/CONF.202/6.

fostering safety initiatives. While most of the identified actions are focused at the United Nations level, the Plan of Action has created key infrastructure within the UN system which can support national level efforts to improve journalist safety. Similar plans of action can also be developed at the national level, either as a governmental effort or a civil society led initiative (see an example of the latter below).

UNESCO is the lead agency for coordinating implementation of the UN Plan of Action. As part of this work, UNESCO has developed a number of resources which are helpful at the national level combatting violence against journalists. Some examples include a set of Journalists' Safety Indicators[469] for both the international and national level, and (with the International Association of Prosecutors) Guidelines for Prosecutors on Cases of Crimes against Journalists.[470]

Philippines: Developing a National Plan of Action

The Philippines has one of the worst records in the world in terms of journalist safety, with 112 journalist deaths recorded by UNESCO since tracking started in 1993.[471] In response, in 2019 a coalition of civil society groups and media organisations launched the Philippine Plan of Action on the Safety of Journalists. The Plan was developed following extensive multi-stakeholder consultations with media, government, civil society and other actors at both the national and local levels.

The Plan sets out a five-year implementation strategy, led again by a multi-stakeholder coalition developed out of the consultation process. Key action points proposed in the Plan include:

- Work to create an independent Press Council.
- Work to create journalist workers' associations.
- A range of actions related to improving occupational, health and safety standards and laws for media workers.
- Institutionalise regular dialogues between state security forces and the media.
- Improve capacities for reporting on and responding to threats against journalists.
- Broaden journalist safety training.
- Develop a gender sensitivity programme for journalists.
- Set up systems for documenting attacks on female journalists.
- Develop protection programmes for university campus journalists.
- Review and reform criminal laws which endanger freedom of expression.
- Create a legal support mechanism for journalists.
- Develop knowledge products on relevant cultural and traditional practices.

[469] UNESCO, 'Journalists Safety Indicators', https://en.unesco.org/themes/safety-journalists/journalists-safety-indicators.
[470] UNESCO and International Association of Prosecutors, 'Guidelines for Prosecutors on Cases of Crimes against Journalists' (2020) (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000375138).
[471] UNESCO Observatory of Killed Journalists, https://en.unesco.org/themes/safety-journalists/observatory.

- Increase public awareness about the role of the media.
- Strengthen the ability of teachers to teach about journalist safety in schools.
- Undertake a study to identify effective safety practices.

The Philippines has also had some government-led safety initiatives over the years, but this initiative is a good example of the range of actions a civil-society led coalition can undertake, even in the absence of clear government leadership.

CONCLUSION

The problem of violence against journalists, and impunity for such crimes, is a complex and pernicious one. In addition, the digital era has created significant new challenges and altered the forms of violence experienced by journalists, especially female journalists. On the other hand, international standards around safety of journalists are well-developed and significant international attention to the issue, such as within the United Nations, means a wide range of resources are now available to governments seeking to find ways to protect journalists better.

Lawyers looking to use litigation as a tool for addressing violence against journalists may consider cases where government actors themselves perpetuate violence. However, international standards also clearly place obligations on States to take action in response to violence against journalists committed by non-State actors. Litigation may therefore be an option for challenging government inaction in the face of such attacks.

MODULE 11: INTRODUCTION TO UN MECHANISMS

- **The United Nations has several mechanisms that contribute to the promotion of human rights, including treaty bodies tasked with overseeing the implementation of core human rights treaties.**
- **UN treaty bodies may consider individual complaints against states that have recognised their jurisdiction to do so.**
- **The UN Human Rights Committee (UNHRCtte) is the treaty body most relevant to freedom of expression and digital rights claims.**
- **Another mechanism of particular relevance is the special procedures, including the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.**

INTRODUCTION

While human rights activism has long been a feature of human society in many different forms, the internationalisation of that movement only truly took root when the United Nations General Assembly adopted the Universal Declaration of Human Rights[472] (UDHR) on 10 December 1948. This document was at least in part motivated from a desire to avoid, as noted in its preamble, "barbarous acts which […] outraged the conscience of mankind" during the Second World War. The UDHR was a landmark statement of the basic civil, political, economic, social and cultural rights to which all human beings are entitled. However, the UDHR is not legally binding because it is a declaration. Two subsequent legally binding instruments were eventually elaborated, namely the International Covenant on Civil and Political Rights[473] (ICCPR) and its two Optional Protocols, and the International Covenant on Economic, Social and Cultural Rights[474] (ICESCR). The ICCPR, UDHR and ICESCR form the International Bill of Human Rights. Numerous other treaties, such as the Convention Against Torture and Other Forms of Cruel, Inhuman or Degrading Treatment[475], have also been developed under the auspices of the United Nations. The United Nations has a variety of mechanisms to encourage compliance with the human rights guaranteed under these instruments. This Module presents an overview of these mechanisms with a focus on treaty bodies and the special procedures system.

[472] United Nations, Statute of the International Court of Justice, 18 April 1946.
[473] UN General Assembly Resolution 2200A (XXI), adopted 16 December 1966, in force 23 March 1976.
[474] UN General Assembly Resolution 2200A (XXI), adopted 16 December 1966, in force 3 January 1976.
[475] UN General Assembly Resolution 39/46, Annex, A/39/51 (1984), 1465 UNTS 85, adopted 4 February 1985, in force 26 June 1987.

Treaty Bodies[476]

In order to monitor and encourage implementation of human rights obligations under UN treaties, a number of committees of independent experts known as 'treaty bodies' were created under various human rights treaties to monitor the implementation of obligations under the treaties over which they have jurisdiction.

Treaty Bodies and Corresponding Conventions

Treaty	Corresponding Treaty Body
International Convention on the Elimination of All Forms of Racial Discrimination	Committee on the Elimination of Racial Discrimination
International Covenant on Economic, Social and Cultural Rights	Committee on Economic, Social and Cultural Rights
International Covenant on Civil and Political Rights	Human Rights Committee
Convention on the Elimination of All Forms of Discrimination against Women	Committee on the Elimination of Discrimination against Women
Convention against Torture and Other Cruel, Inhuman or Degrading Treatment	Committee against Torture
Convention on the Rights of the Child	Committee on the Rights of the Child
International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families	Committee on Migrant Workers
Optional Protocol of the Convention against Torture	Subcommittee on Prevention of Torture and other Cruel, Inhuman or Degrading Treatment or Punishment
International Convention on the Rights of Persons with Disabilities	Committee on the Rights of Persons with Disabilities
International Convention for the Protection of All Persons from Enforced Disappearance	Committee on Enforced Disappearances

The exact mandates of the treaty bodies vary, but they share many features. Each treaty body, with the exception of the Subcommittee on the Prevention of Torture:[477]

- Considers regular reports on respect for treaty rights which are submitted by State parties;

[476] For more information on treaty bodies, see International Service for Human Rights, 'Simple Guide to the UN Treaty Bodies' (2015) (accessible at: https://ishr.ch/defenders-toolbox/resources/updated-simple-guide-to-the-un-treaty-bodies-guide-simple-sur-les-organes-de-traites-des-nations-unies/)

[477] The Subcommittee on the Prevention has a distinct preventative mandate and is different from the Committee against Torture, the mandate of which more closely resembles that of other treaty bodies.

- Publishes observations and recommendations to guide specific states in implementing their obligations under the treaty; and
- Elaborates and publishes 'general comments', which are authoritative interpretations of specific articles or subject matters covered in their treaty.[478]

Additional activities that certain treaty bodies are mandated to perform include considering and issuing opinions on individual and (more rarely) inter-state complaints and conducting or initiating investigations through country visits.[479]

The Human Rights Council

The Human Rights Council is a UN intergovernmental body, with a mandate to promote human rights compliance. The Council was created in 2006 through a UN General Assembly resolution[480] as a replacement for the UN Human Rights Commission in response to perceived failings of that body.[481] The Human Rights Council consists of 47 states elected for fixed terms "based on equal geographical distribution."[482]

The Human Rights Council holds three regular sessions annually, in addition to certain 'special sessions' held to address urgent human rights situations.[483] A key outcome of many of these sessions are Human Rights Council resolutions addressing thematic issues or pressing country-specific situations. Although non-binding, these resolutions often have significant persuasive force and have helped contribute to the progressive development of human rights standards. However, as the direct product of an intergovernmental body, they are inevitably influenced by certain political considerations and are sometimes the product of compromises due to the need to build sufficient support among the states which sit on the Council.

One prominent mechanism associated with the UN Human Rights Council is the Universal Periodic Review (UPR) process. The UPR is a process whereby states undergo regular reviews of their human rights record. Previously, this occurred every four years although the review has moved to a four-and-a-half-year schedule.[484] The UPR is based on a consultative and cooperative process whereby reviewed states present a report and other states are afforded the chance to provide comments, questions and recommendations.[485] Civil society cannot directly participate in the review, although

---

[478] International Service for Human Rights, 'Simple Guide to the UN Treaty Bodies', above n 5, p. 14.
[479] *Id.*
[480] UN Doc. A/RES/60/251(2006) (accessible at: http://www.un-documents.net/a60r251.htm).
[481] For more background on the impetus for creating the Human Rights Council, see Rosa Freedman, 'The Human Rights Council' in Philip Alston and Frédéric Mégret (eds.), *The United Nations and Human Rights: A Critical Appraisal*, 2nd ed (2020, Oxford University Press).
[482] GA Res 60/251 (2006), above n 5 at para. 7.
[483] Child Rights International, 'A Guide to UN Human Rights Mechanisms' at p. 5 (accessible at: https://static1.squarespace.com/static/5afadb22e17ba3eddf90c02f/t/60d1e2790208354614305583/1624367738499/UN+mechanisms_+A+guide_2015.pdf).
[484] Rosa Freedman, 'The Human Rights Council' in Philip Alston and Frédéric Mégret (eds.), above n 10 at p. 220.
[485] For more on the UPR process, see Office of the High Commissioner for Human Rights, 'Universal Periodic Review' (accessible at: https://www.ohchr.org/en/hr-bodies/upr/upr-main).

non-governmental organisations may observe proceedings, provide submissions and suggest questions be put forward by states which with they may have good relations.[486]

Another key mechanism mandated by the UN Human Rights Council is the special procedures system. The special procedures are mandates created to address thematic or geographic issues and take the form of individuals (either Special Rapporteurs or Independent Experts) or Working Groups consisting of five members drawn equally from five different regional groups.[487] These special mechanisms engage in a variety of activities, such fact-finding, country missions and reporting, publishing thematic reports, addressing UN bodies, and receiving and following up on individual communications.

The Principal Organs of the United Nations

The principal organs of the UN (the General Assembly, the Economic and Social Council, the Security Council and the International Court of Justice) all play a role in the UN human rights system. The General Assembly is the primary deliberative body of the UN and regularly issues non-binding resolutions, many of which address country-specific or thematic human rights issues. Also of relevance to human rights are the activities, such as debates and resolutions, of certain subcommittees of the General Assembly, notably the Third Committee (which covers social, humanitarian and cultural matters) and the Sixth Committee (which covers legal affairs).[488] The human rights activities of the Economic and Social Council have waned over the years, although it still plays a role in respect of economic, social and cultural rights, including preparing reports and recommendations in relation to these rights.[489]

In contrast to the Economic and Social Council and the General Assembly, the Security Council can in certain cases issue resolutions that are formally binding as a matter of international law. Although the Council is not in essence a human rights body, certain matters of peace and security inevitably involve human rights issues (for example, in respect of peacekeeping missions that include a human rights mandate or serious situations of human rights abuse which are deemed to pose a threat to security).[490] The International Court of Justice is the UN's main judicial organ. Its decisions are formally legally binding on states that have accepted the jurisdiction of the Court. Although the International Court of Justice is not a human rights court and not mandated to accept individual complaints, some of its decisions have played a key role in the development of international human rights jurisprudence.[491]

---

[486] For more information on civil society participation in this process, see Office of the High Commissioner for Human Rights, 'Universal Periodic Review: a Practical Guide for Civil Society' (2014) (accessible at: https://www.ohchr.org/en/publications/universal-periodic-review-practical-guide-civil-society).
[487] *Id.* at p. 229.
[488] See Andrew Clapham, 'The General Assembly' in Philip Alston and Frédéric Mégret (eds.), above n 10, pp. 104-105. For more background on the General Assembly, see Council on Foreign Relations, 'Backgrounder: The Role of the UN General Assembly' (2021) (accessible at: https://www.cfr.org/backgrounder/role-un-general-assembly).
[489] Frédéric Mégret, 'The Economic and Social Council' in Philip Alston and Frédéric Mégret (eds.), above n 10 at p. 132.
[490] On the role of the Security Council in human rights protection, see Bardo Fassbender (ed.), *Securing Human Rights?: Achievements and Challenges of the UN Security Council* (2012, Oxford University Press).
[491] On the role of the International Court of Justice in human rights protection, see Eva Rieter, 'The International Court of Justice and Its Contribution to Human Rights Law: Final Report of the ILA International Human Rights Law Committee', pp. 19-15 of *Judging International Human Rights* (2019, Springer).

The Office of the High Commissioner for Human Rights

The UN Office of the High Commissioner for Human Rights (OHCHR) has a coordinating role in respect of the UN's human rights activities and works closely with the various UN bodies, including the treaty bodies, the UN Human Rights Council and the special procedures, as well as working directly with states to encourage compliance with human rights norms. Of particular use for legal practitioners is the OHCHR's centralised database of the jurisprudence of human rights treaty bodies.

RECOURSE UNDER TREATY BODIES

Individual Complaints

One of the key activities of many treaty bodies is considering individual complaints (also known as petitions or individual communications) from rights holders or their duly appointed counsel. Through these complaints, the treaty bodies consider allegations by petitioners that a state has violated its treaty obligations. After hearing from the petitioner and responses from the concerned state, the treaty body issues its decision, formally called 'views', on whether or not the petitioners' claims of a human rights violation are made out and makes a recommendation.[492] The treaty bodies' recommendations are not formally (legally) binding, but their bodies' views have considerable normative weight.[493]

Currently the complaint mechanisms of eight treaty bodies have entered into force, namely:

- The Human Rights Committee
- The Committee on Elimination of Discrimination against Women
- The Committee against Torture
- The Committee on the Elimination of Racial Discrimination
- The Committee on the Rights of Persons with Disabilities
- The Committee on Enforced Disappearances
- The Committee on Economic, Social and Cultural Rights
- The Committee on the Rights of the Child

For a complaint to be admissible, the state must have accepted the jurisdiction of the treaty body over individual complaints. The mechanism for authorising this differs according to the treaty. For example, in the case of the ICCPR, the individual complaints mechanism is contained in the (first)

[492] Office of the High Commissioner for Human Rights, 'Individual Complaint Procedures under the United Nations Human Rights Treaties', Fact Sheet No. 7/Rev.2 (2013) at p. 10 (accessible at: https://www.ohchr.org/sites/default/files/2021-08/FactSheet7Rev.2.pdf).

[493] The UN Human Rights Committee describes its views as 'authoritative determinations' and refers to the right to a remedy and the obligation of state parties to act in good faith in relation to their obligations under the ICCPR in underscoring the need for state parties to cooperate with the Committee. See Human Rights Committee, 'General comment No.33: Obligations of States parties under the Optional Protocol to the International Covenant on Civil and Political Rights', UN Doc. CCPR/C/GC/33 (2009) at paras. 13-15 (accessible at: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no33-obligations-states-parties).

Optional Protocol to the ICCPR. As a result, it is only where a state has ratified the Optional Protocol that the Committee is authorised to consider individual communications against that state. For other committees, the procedure through which individual complaints are authorised is contained within the core human rights treaty. For example, for the Committee against Torture to consider complaints, the relevant state must have recognised the Committee's competence over individual complaints through a declaration made under Article 22 of the Convention against Torture.

The UNHRCtte will likely be the Committee best placed to consider complaints about digital rights and freedom of expression issues because this right (and the right to privacy) is explicitly guaranteed in the ICCPR. However, other treaty bodies may also be appropriate for such a complaint. For example, in cases involving freedom of expression of children, complainants may consider making a complaint to the Committee on the Rights of the Child, which oversees the Convention on the Rights of the Child, which also guarantees freedom of expression for children. A violation of freedom of expression may have gendered other discriminatory aspects, in which case a complaint may be appropriate to, respectively, the Committee on Elimination of Discrimination against Women or the Committee on the Elimination of Racial Discrimination.

When deciding whether to make an individual complaint to a UN treaty body, the following considerations should be kept in mind:

- It is important first to determine the state which is responsible for the alleged human rights violation. Usually, this is straightforward. However, the transnational nature of digital rights issues may mean that this requires some consideration. For example, a complaint might involve states' failure to fulfil positive obligations in relation to private actors that may have connections to more than one jurisdiction.
- Petitioners must determine which treaty bodies have geographical jurisdiction (known as competence *ratione loci*) over the complaint. A useful tool for this is the OHCHR's interactive dashboard, which lists the status of human rights treaty ratifications for UN member states.[494] For example, the Maldives, Nepal, the Philippines and Sri Lanka are parties to the (first) Optional Protocol to the ICCPR, and thus recognise the competence of the UNHRCtte over individual communications.[495]
- Where a state party accepts the jurisdiction of different treaty bodies, thought should be give to the most effective way to pursue a complaint, as one of the general criteria for the admissibility of complaints to treaty bodies is that no complaint regarding the same matter may be pending before another international body.[496] A key consideration as to which committee to choose will be which violation is most central to the complaint. However, at a practical level, counsel may consider whether different treaty bodies have different processing times, in view of the lengthy backlogs of certain committees of up to several

[494] In order for this resource to be useful, counsel must, however, be familiar with the way the authorisation to consider an individual communication is made, for example, through an optional protocol or a declaration directly under the treaty.
[495] Office of the High Commissioner for Human Rights, 'Ratification Status for CCPR-OP1 - Optional Protocol to the International Covenant on Civil and Political Rights' (2022) (accessible at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR-OP1).
[496] See, for example, Article 5(2)(a) of the Optional Protocol to the ICCPR, which provides that the Human Rights Committee must determine that "the same matter is not being examined under another procedure of international investigation or settlement".

years to process individual complaints. Information on processing times may be inferred from the annual reports of the treaty bodies.[497] Despite the lengthy backlog of many treaty bodies, when complaints involve particularly urgent matters, petitioners may be able to apply for 'interim measures', whereby a treaty body requests that a state refrain from taking certain actions to avoid 'irreparable damage' before the underlying complaint is considered on its merits.[498]

- For complaints to be deemed admissible, petitioners must generally be able to show that domestic remedies have been exhausted, although there are some exceptions, for example, where no effective or realistic domestic remedy is available. In addition, complaints should be submitted as soon as possible after the exhaustion of domestic remedies, with certain treaty bodies specifying an exact time limit.[499] For the UNHRCtee, there is no absolute cut off. However, "a communication may constitute an abuse of the right of submission, when it is submitted five years after the exhaustion of domestic remedies by the author of the communication, or, where applicable, three years from the conclusion of another procedure of international investigation or settlement, unless there are reasons justifying the delay, taking into account all the circumstances of the communication."[500]
- Another criterion of admissibility is that the treaty body must have temporal competence over the complaint (known as *ratione temporis*). This generally means that the violation occurred after the relevant instrument came into force for the state party. However, treaty bodies may also have jurisdiction over a 'continuous violation', defined by the Human Rights Committee as "an affirmation, after the entry into force of the Optional Protocol, by act or by clear implication of the previous violations of the State party."[501]
- The complainant must have standing to bring a complaint. In contrast to strategic litigation involving public interest litigants before domestic courts and some regional human rights courts, the UNHRCtte requires complainants be actually, personally aggrieved human beings

---

[497] For example, the Human Rights Committee's 2020 annual report indicates a significant backlog before that Committee, noting that in 2020 155 cases were concluded and 1,193 cases remained pending by 31 December 2020. See 'Report of the Human Rights Committee to the General Assembly', UN Doc. A/76/40 (2021) at para 24 (accessible at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=A%2f76%2f40&Lang=en).

[498] For an application of interim measures in the context of freedom of expression (specifically the UN Human Rights Committee's request not to destroy a painting), see Human Rights Committee, *Shin v. Republic of Korea*, Communication 926/2000 (2004), UN Doc. CCPR/C/80/D/926/2000 at para. 1.2 (2004) (accessible at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f80%2fD%2f926%2f2000). For more on interim measures, see Helen Keller and Cedric Marti 'Interim relief compared: use of interim measures by the UN Human Rights Committee and the European Court of Human Rights', Max-Planck-Institut, ZaöRV 73 (2013) (accessible at: https://www.researchgate.net/publication/278752013_Interim_relief_compared_use_of_interim_measures_by_the_UN_Human_Rights_Committee_and_the_European_Court_of_Human_Rights).

[499] International Service for Human Rights, 'Simple Guide to the UN Treaty Bodies', above n 5, p. 26.

[500] UN Human Rights Committee, Rules of Procedure (2021), UN Doc. CCPR/C/3/Rev.12 at R 99(c) (accessible at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=65).

[501] *Könye v. Hungary*, Communication 520/1992, UN Doc. CCPR/C/50/D/520/1992 (1994) at para 6.4 (accessible at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2F50%2FD%2F520%2F1992).

and does not permit public interest actions (known as '*actio popularis*').[502] Corporations and other non-human entities do not have standing to make complaints before that Committee,[503] although groups of similarly impacted individuals may submit a collective complaint.[504] The petition can be made by the person or persons alleging the violation(s) or through a duly appointed representative.

The above considerations are generally applicable to the individual complaint process before treaty bodies. However, counsel must do their own research when deciding whether to bring forward and in drafting individual complaints and should consult the specific admissibility criteria of the relevant treaty body. The most up-to-date version of the relevant UN treaty body's rules should be consulted, along with any relevant case law of the treaty body, as well as the text of the treaty and any relevant protocols. Complaints should explicitly outline how they meet all criteria for admissibility and clearly identify which articles are alleged to have been violated and the remedy or remedies sought. It is helpful to refer in submissions to any pertinent case law of the treaty body, as well as any pertinent general comments, such as the UNHRCtte's General Comment No. 34, which focuses on freedom of expression.[505]

Treaty body reviews

Another key function of treaty bodies is the obligation to report regularly, whereby state parties are required to report periodically on their performance in terms of their progress or lack thereof in terms of respecting treaty rights. Once a state has lodged its initial report, there is a process of review involving the oversight treaty body, which ends up with the latter publishing a report with their observations on the status of the state's implementation of treaty obligations and recommendations for improvements. There are opportunities for civil society members to play a role in this process as the treaty bodies invite submissions. As a result, where a state is a party to a human rights treaty, rights-holders may be able to bring their concerns to the relevant treaty body when their state is up for review, even if it has not recognised the treaty body's jurisdiction over individual complaints.[506]

---

[502] *S.B. v. Kyrgyzstan,* Communication No 1877/2009, UN Doc. CCPR/C/96/D/1877/2009 (2009) at para. 4.2 (accessible at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f96%2fD%2f1877%2f2009).
[503] See, for example, *Lamagna v. Australia*, Communication No 737/1997, U.N. Doc. CCPR/C/65/D/737/1997 (1999) at para. 6.2 (accessible at: http://hrlibrary.umn.edu/undocs/session65/view737.htm).
[504] *Kitok v. Sweden*, Communication No 197/1985, UN Doc. CCPR/C/33/D/197/1985 (1988) (accessible at https://juris.ohchr.org/Search/Details/543).
[505] 'General Comment No. 34: Article 19: Freedoms of opinion and expression' (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[505] CCPR/C/103/D/1815/2008/Rev.1 (2008) (accessible at https://juris.ohchr.org/Search/Details/1613
[506] For background on the Human Rights Committee's treaty body review process, see Office of the High Commissioner for Human Rights, 'Guidelines and tools for treaty body reporting' (2022) (accessible at: https://www.ohchr.org/en/treaty-bodies/guidelines-and-tools-treaty-body-reporting).

RECOURSE UNDER THE SPECIAL PROCEDURES

Another way to raise human rights concerns before the UN is through communications to the UN's independent experts (the Special Procedures), which consist of both thematic and country mandates.

Of particular relevance here is the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, a position that was first mandated in 1993.[507] The Special Rapporteur undertakes a number of activities in support of freedom of expression, including engaging in fact-finding country visits, preparing thematic reports, responding to individual communications and preparing urgent appeals to states on alleged violations.[508] In addition to receiving communications about urgent cases, the Special Rapporteur periodically issues calls for input into thematic reports and welcomes relevant submissions from members of civil society. Another Special Rapporteur of particular relevance to digital rights is the UN Special Rapporteur on the right to privacy, who undertakes similar tasks to help advance privacy rights.

Often in cases of cross-cutting human rights concerns, special rapporteurs issue joint statements. For example, in June 2021, the Special Rapporteur on freedom of expression, the Special Rapporteur on freedom of peaceful assembly and association, and the Special Rapporteur on the right to privacy issued a joint communication to India highlighting human rights concerns with newly published rules issued under India's Information and Technology Act.[509]

Certain working groups may also provide freedom of expression recourse in some circumstances. For example, freedom of expression issues sometimes involve arbitrary detentions and, in such cases, individuals or their counsel may consider a complaint to the Working Group on Arbitrary Detention.[510]

CONCLUSION

Although there is not yet a regional human rights court in South or Southeast Asia, and only a limited human rights system in Southeast Asia (and none in South Asia), the UN human rights system can still play an important role in upholding human rights in these regions. Among the most effective tools that individual rights-holders may have is to bring, directly or through their counsel, individual complaints to treaty bodies. Another tool that is not dependent on states' having accepted the jurisdiction of treaty bodies in relation to individual complaints is to raise concerns through communications with the UN special procedures, notably the UN Special Rapporteur on freedom of expression and the Special Rapporteur on the right to privacy. Engagements with states by the UN

---

[507] For more the Special Rapporteur, see Office of the High Commissioner for Human Rights, 'About the mandate: Special Rapporteur on freedom of expression and opinion' (2022) (accessible at: https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/about-mandate).
[508] *Id.*
[509] Communication OL IND8/2021 (2021) (accessible at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385).
[510] For background on the jurisprudence of this Working Group, see Jared Genser, *The UN Working Group on Arbitrary Detention: Commentary and Guide to Practice* (2020, Cambridge, Cambridge University Press) (accessible at: https://www.perseus-strategies.com/wpcontent/uploads/2020/04/Jared-Genser-The-UN-Working-Group-on-Arbitrary-DetentionCambridge-University-Press-2019.pdf)

treaty bodies and special procedures can prove highly impactful for those seeking to hold their states to account for rights violations, whether in individual cases or more generally.