# National Human Rights Institutions in Digital Spaces

Author: Gayatri Khandhadai

Editor: Deborah Brown

For the Association for Progressive Communications

## 1. Introduction

Increasingly, people across the globe and more particularly in Southeast Asia are relying on the internet to interact, communicate, work, learn and realise their rights. Similarly, states are also relying on the internet and digital tools to deliver services and improve the overall functioning of the government through e-governance[1] initiatives. As this shift unfolds before us, we are forced to adapt our focus and the way we work to ensure that all people are able to enjoy and exercise all rights across all platforms, including though information and communication technologies (ICTs).

Recognising the potential of ICTs, the ASEAN ICT Masterplan 2020 states: 'Information and Communications Technology (ICT) has played a critical role in supporting regional integration and connectivity efforts. And as the region forges ahead to further deepen economic integration and community building, ICTs are expected to play an increasingly pivotal role' (ASEAN, 2015: 7).

The Masterplan recognised that ICTs, and in particular the internet, have become a core part of the economy and embedded infrastructure, progressively underlying all aspects of socio-economic growth and development. It identified eight areas as strategic thrusts: Economic Development and Transformation, People Integration and Empowerment through ICT, Innovation, ICT Infrastructure Development, Human Capital Development, ICT in the ASEAN Single Market, New Media and Content, and Information Security and Assurance. Each of these areas has a potential impact of furthering people's civil, cultural, economic, political and social rights. It

1 Electronic governance or e-governance is the application of information and communication technology (ICT) for delivering government services, and the exchange of information, among other functions.

would therefore be crucial to address these areas of strategic thrust from a human rights perspective.

The rapid development of ICTs, and the spread of services and applications that make use of them, has been one of the most important developments in human society over the past 30 years. Four aspects of this have been particularly significant where rights are concerned, namely computerisation, telecommunications, the internet and online social networks (Souter, 2013). For those who have access to the internet, it is becoming increasingly difficult to imagine life without it. It offers people all kinds of opportunities, including exercising our human rights both online and offline, as different UN Human Rights Council resolutions have established.[2] In fact, the UN Human Rights Council and the UN Human Rights Committee have recognised the applicability of human rights in the digital environment, and through Special Procedures, resolutions and general comments, they have elaborated on states' responsibilities for upholding human rights online.

National human rights institutions (NHRIs) are now, beyond a doubt, valued as essential actors in the task of protecting and promoting human rights at the national and regional levels. To this end, they must work with one another to meet evolving developments and challenges in the exercise of human rights by all. As more people rely on ICTs to realise their rights, and as states are increasingly moving to regulate the internet, NHRIs must take a proactive approach to ensure that this new space remains an enabling one for the exercise of human rights.

ICTs also offer NHRIs the potential to be more effective and reach citizens, but in doing so, they must remain aware of the security risks or concerns involved for them and their constituencies. The exercise of human rights by individuals through ICTs not only impacts their experience of these rights in the online space; it can also have a significant impact offline, both positively and negatively. NHRIs must therefore, in accordance with their mandate of defending human rights, work towards addressing, promoting and protecting human rights exercised by all individuals on all platforms, including online.

## 2. NHRIs and digital tools

[2] For example, UN Human Rights Council resolutions 20/8, 24/5, 26/13 and 32/13.

ICTs and more specifically, the internet create new and promising spaces where NHRIs can improve the way they function and reach out to stakeholders in previously unimaginable ways. Digitalisation has fundamentally changed the way we work. NHRIs can develop practices that systematically help them record and store information about their work in digital form. Similarly, digital tools, like email, chat applications and video conferencing, help NHRIs function more efficiently and save on precious resources spent on physical infrastructure. For instance, NHRIs can use online collaborative platforms to work with their staff and partners situated remotely (Association for Progressive Communications, 2011). Similarly, using web-based audio, video and text communication tools can help save on communications costs for NHRIs. However, it should be emphasised that NHRIs must not completely move away from existing offline platforms and mechanisms. This is to ensure that the people who are not able to meaningfully access and use the internet, for reasons of infrastructure, cost, skills, or social and cultural barriers, are not left behind and thus further marginalised. Segments within society who need the attention and protection of NHRIs often experience digital exclusion. To this end, NHRIs also have the responsibility of reminding governments that their obligation to protect, promote and fulfil all human rights includes providing meaningful access to the internet to all people.

The internet also enables NHRIs to reach out to their stakeholders, including citizens and the state, more effectively and directly. A well-resourced, updated and interactive website can help facilitate two-way communication between NHRIs and different stakeholders. NHRI websites must carry broad information on who they are, what their mandate covers, what services they offer to the public, the structure of the organisation, current and past areas of work and initiatives, reports, plans, policies and contact information. In principle, NHRIs should make all available information public through their websites, unless there is good reason to withhold certain information, in accordance with national and international freedom of information standards.

Websites of NHRIs should be accessible and understandable in form and content. They must be designed bearing in mind that the Web is fundamentally designed to work for all people, whatever their hardware, software, language, culture, location, or physical or mental ability. For instance, NHRIs should consider the need to have their websites available in multiple languages, depending on the linguistic makeup of their respective states. Also, the website must be accessible to people with a diverse range of hearing, movement, sight and cognitive ability challenges. To this end, NHRIs must strive to ensure that their websites meet the standards prescribed by the

World Wide Web Consortium (W3C),[3] which are widely accepted and followed as good practices by states.

Another key use of the website is in ensuring that people and interest groups are able to invoke the protection mandate of the NHRI by filing complaints or petitions through the digital, online medium. Many NHRIs in Southeast Asia are already providing this option for people.[4] By ensuring that people can file complaints online in addition to offline means, NHRIs will be able to better connect with victims. Online complaints mechanisms should also offer the option of filing anonymous reports, so as to help persons report violations without fear of repercussions or reprisals. Further, this should be accompanied by means to submit digital evidence or corroborating documents, with clear internal guidelines on how to deal with digital evidence.[5] Online complaints mechanisms can also help victims check on the status of their complaints directly, instead of having to petition the NHRI each time to learn about the progress.

A prominent online presence for NHRIs through social media can contribute to improving their proximity to victims as well as actively promoting human rights and monitoring the environment for violations, online and offline. By engaging with individuals, media and civil society through social media, NHRIs can establish a direct relationship. However, being more active on social media also means being more vulnerable to undesirable comments, threats and confrontations. While this might be a difficult adjustment, over the long run it will turn out to be a substantial aid. For instance, being active on Twitter and Facebook by constantly sharing updates and information on the NHRI's activities would help garner support for its work and integrate it within the larger movement for human rights more obviously. People's reactions will also help NHRIs remain aware of the expectations of different groups, even if these cannot always be met. This can be particularly helpful when an NHRI has to take a position against the state or is facing reprisals from the state as a result of its work. NHRIs will be able to garner support among individuals and civil society on social media in these instances, and this lends to the legitimacy and protection for the NHRIs themselves. Being active on social media also lets NHRIs put out

[3] For more information, visit the World Wide Web Consortium website: https://www.w3.org/Consortium

[4] Including NHRIs in Malaysia, Timor-Leste, Thailand and Indonesia.

[5] For a comparative analysis of how digital evidence is received in European jurisdictions, please see Mason, 2016.

timely and immediate reactions to grave violations. NHRIs coming out in support of victims on social media will also make the victims and interest groups feel supported.

Further, with most media outlets turning digital, monitoring the news for both online and offline violations becomes easier for NHRIs. In many cases, instances of violations are first reported by people on social media before they hit newspapers. By being diligent online, NHRIs will be able to get updated information and diverse accounts of what happened. However, NHRIs must continue with their traditional forms of monitoring in parallel, as in many places access to the internet and digital inclusion remain a challenge.

The data collected through the websites, online complaints mechanisms, monitoring and social media can be used, in addition to data collected offline, to inform annual or periodic reports of NHRIs. For instance, NHRIs can provide aggregated data on the number of visitors to their website and compare it to previously recorded figures. This could help indicate the presence and reach of the NHRI. Data on the gender of complainants could also help indicate whether the NHRI is able to cater to the needs of different gender groups. By tagging the complaints under different categories, NHRIs will be able to determine what forms of violations are more prominently reported through the complaints mechanism. While all of this can be done through offline mediums as well, using online tools promotes efficiency and aids in the process of doing in-depth analysis.

## 3. Security: What is at risk for NHRIs operating online[6]

While working online and using ICTs can expand the impact of NHRIs considerably, this also requires NHRIs to be aware of vulnerabilities that come with such use and the need to adopt good practices. A strong online presence comes with a responsibility to ensure the security and rights of NHRI staff, partners and beneficiaries.

Threats to the rights of NHRI staff, partners and beneficiaries range from website and database hacking, compromising online communications, leaking or theft of sensitive private or personal information, to becoming victims of social, corporate or government-sponsored surveillance and online or offline abuse.

[6] This section was prepared by Gayatri Khandhadai, Mallory Knodel and Furhan Hussain.

### *Digital security: Unpacking the term and basic practices*

In the present age, it is essential that all operations and activities undertaken by NHRIs in online and offline spaces take into account good practices for digital security. Digital security is the protection of information and digital identity akin to protection and security in the offline realm. Digital security also refers to a system or a set of practices for securing information and digital identities to prevent harm or undesirable access or use. Digital security includes the use of behaviours and tools in online and offline spaces that lead to the securing of identity, assets and technology. Existing resources such as Security in a Box[7] and the Digital Security First Aid Kit[8] are a good starting point for NHRIs to explore what is at risk and what measures can be adopted to deal with or pre-empt threats.

Contrary to common understanding of the subject, digital security does not necessarily require advanced knowledge of computing technologies. Rather, it requires a thorough understanding of daily work processes and procedures, and a sense of how information is stored or transferred from one person or device to another. This helps the organisation and its staff identify potential vulnerabilities and data leaks, and triggers a process of behavioural change that results in the strengthening of the NHRI's overall information security. For instance, by exploring what passwords are and how they function, NHRIs can come to the conclusion that simply by increasing the length and complexity of a set of characters in a password, an information system's defence can be significantly improved against brute force attacks.[9] This approach to security is also more practical as it helps the organisation identify existing resources to address vulnerabilities rather than thinking only of solutions that can be provided by external actors or experts, which may be expensive and thereby prove to be a barrier. However, to maintain a robust digital security environment, it is recommended that NHRIs consider investing in updated security systems.

---

[7] Available at https://securityinabox.org/en/

[8] Available at https://www.apc.org/en/irhr/digital-security-first-aid-kit

[9] A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In an attack of this kind, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. For more details, please see: https://www.techopedia.com/definition/18091/brute-force-attack

### *Internal risks and mitigation for individuals*

Upholding human rights is a challenging task where security threats online and offline may result from political interests and power players. NHRI members, staff, witnesses and sources can be targets of governments and third parties online. NHRIs must determine what data they need to protect in their investigation of human rights violations, and whom they need to protect it from, in order to keep it secure from unauthorised access and abuse.

Though NHRIs enjoy the status of carrying a legal mandate and some level of protection from the state, the organisational approach should always favour proactive measures for establishment of security practices, rather than reactive ones. In order to ensure this, human resources and ICT management within NHRIs may need to assess job roles as well as risk factors of individual staff members in order to devise individual risk mitigation plans in a proactive manner.

### *Information systems and risks*

Any information management systems for NHRIs that are connected to and accessible over the internet are vulnerable not only to malicious acts such as hacking, defacement or distributed denial of service (DDoS) attacks;[10] they can also be compromised unintentionally through human error or network failures. To mitigate outages, careful risk reduction and contingency planning must be put into place to ensure that staff can communicate with one another, do their work and keep critical lines of communication open with the rest of the world.

Similarly, threats to information can happen both accidentally or maliciously. For instance, data storage mediums can be damaged or corrupted. Hackers can hold a device server hostage for ransom through hacking or a malware attack. It is important to assess and mitigate these threats to institutional knowledge and data by taking steps such as backing up data on both shared systems as well as external physical storage devices such as disks. While doing so, it is advisable to use

[10] A 'denial of service' attack is where malicious users crowd out legitimate users of a service such as a website or a chat server. In a 'distributed' denial of service (DDoS), attackers use thousands of machines under their control to target a site. For more details, please visit: https://www.digitaldefenders.org/digitalfirstaid/sections/research

devices that support encryption so as to protect sensitive information and data from being accessible to unauthorised persons.

Here, it must be emphasised that digital security cannot be achieved by only focusing on the security of information and systems. It is also about the physical security of digital devices and the persons that have access to them. This comes from acknowledging that the device as well as the data it contains are important. Data stored in a digital device is only as secure as the physical device and its environment. For instance, data on a device that is not encrypted or protected with strong passwords can easily be accessed by anyone who gains control over the device, even if this access is momentary.[11]

***Understanding risks and consequences***

In addition to the inconvenience caused by attacks on systems and information, we must consider the cost of insecure communications and uninformed digital practices on the rights and wellbeing of individuals, as well as the effectiveness and credibility of NHRIs. A few extra steps can go a long way in preventing the inconvenience and potentially dangerous consequences of unsecure practices for the organisation, individuals working in NHRIs, and those with whom they are communicating.

One area that particularly warrants attention relates to the security of information provided through online complaints mechanisms on NHRI websites. While the availability of online complaints mechanisms is a welcome development, NHRIs must also be aware of the risks that come from the data of complainants being vulnerable to cyberattacks. This could put the victims – who are already in a stressful situation – in harm's way, as attackers will be able to see what was said by the complainant and who is assisting the victim to access justice.

Given the nature of their work, NHRIs are entrusted with vast amounts of data which include identifying information of victims, evidence of human rights violations, personal testimonies, and contact details of individuals at high risk. An NHRI's task is to not only work towards protecting high risk persons and groups, but also to ensure that all persons and groups communicating with them do not become victims of attacks as a result of poor information management practices. This

[11] Encryption is illegal in some jurisdictions. NHRIs should check national legislation governing encryption.

is where post-assessment of security needs and practices and a structured and well-planned approach towards implementing digital security are required. To begin, it is essential to design a set of policy guidelines, especially a privacy policy, which is of prime importance.

***Policies and procedures***

A privacy policy is a document that commits to how the NHRI will responsibly monitor, collect, store, disclose and disseminate various forms of information belonging to its staff, partners and beneficiaries. Such an effort goes a long way in ensuring that practical but effective standard operating procedures (SOPs) stem from it and form the basis of all operations pertaining to the use of digital technologies. Similarly, NHRIs should also adopt ICT policies that establish SOPs for communication and information sharing as well as how technology is to be used across the organisation.

From the perspective of security alone, it is important that all organisational management SOPs, including ICT policies, take into account the digital security needs of the NHRI. These include (but are not limited to) procurement, management and disposal of digital devices; use of personal devices and social media for official work; development and maintenance of information systems such as online databases and websites; collection and storage of information; staff access to devices and data; gender sensitivity and consent; security of the NHRI's physical environment; emergency response mechanisms; management of external venues and events; psychosocial support; and capacity building for staff and partners on these issues.

Once policies are in place, NHRIs must strive towards ensuring that they are implemented and that staff receive necessary support and training to adhere to these policies. NHRIs would also need to periodically assess and update their policies and practices to meet the evolving developments in ICTs.

NHRIs must also be cognisant of the vast amounts of information on users that their websites may collect. The security of such a system can only be improved if the online platforms of NHRIs allow an unbroken and secure (SSL/HTTPS) connection, with the option to encrypt the information of users. The website can also be tweaked to never collect user data through cookies and other tracking methods. Further, NHRIs can consider imbedding a step-by-step guide to route

their complaints through a provided virtual private network (VPN) or proxy connection to improve the anonymity of victims using the online complaint mechanisms. These steps allow privacy to be designed into the system by default and minimise potential harm to complainants as a result of accidental disclosure of identity.[12]

As technology rapidly advances, key human rights institutions leaving online spaces unattended could lead to these spaces being suppressed by interests that diminish fundamental rights across the digital world. Keeping this in mind, NHRIs must take the first step towards committing to establish comprehensive ICT and rights-oriented policies and SOPs in order to reclaim online spaces for activism and protection of critical liberties.

## 4. Human rights online

Throughout Southeast Asia and the world, people have taken to online platforms to exercise their rights in ways that were not possible through traditional mediums. The internet's role has become so much more relevant today that many governments have tried to regulate it in ways that threaten citizens' rights.

Since the landmark resolution by the UN Human Rights Council in 2012, which affirmed that the same rights people enjoy offline also apply online,[13] the HRC now considers an internet-themed resolution every two years[14] and has gone from recognising at a fundamental level the applicability of human rights in the online environment, to addressing critical issues like bridging the gender digital divide, attacks on people for exercising their rights online, ending intentional disruptions to internet access, and improving access to the internet and ICTs for persons with disabilities. The most recent resolution was passed in July 2016 and links human rights online to the achievement of the Sustainable Development Goals.[15]

[12] NHRIs should analyse national legislation to see if the use of VPNs is legal in their jurisdiction.

[13] A/HRC/res/20/8, June 2012, available at https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement

[14] A/HRC/res/26/13, June 2014; A/HRC/32/L.20, June 2016.

[15] A/HRC/20/L.13.

Further efforts to concretise internet freedom can be seen in the launch of the Freedom Online Coalition of governments in December 2011,[16] greater prominence and acceptance of human rights as a legitimate topic in the UN Internet Governance Forum (IGF),[17] and events such as the Stockholm Internet Forum.[18]

A key indicator that human rights on the internet has become a discussion integrated within human rights mechanisms in the UN is the significant number of submissions by stakeholders to the Universal Periodic Review process[19] and the corresponding recommendations made by states to one another on issues relating to human rights online (Brown & Kumar, 2016).

Some obvious and prominent civil and political rights exercised on and impacted by the internet include freedom of expression, religion or belief, assembly and association. Economic, social and cultural rights such as the right to health, education, culture and work also form a significant area of focus (Esterhuysen, 2016). In terms of stark violations, online harassment and gender-based violence, particularly those experienced by women and individuals who face discrimination based on their sexual orientation and gender identity, warrant attention by NHRIs. Laws and policies implemented by states comprise another key area of focus for NHRIs, as they impact on the ability of people to exercise human rights online and legitimise restrictions.

### *Freedom of expression*

Freedom of expression[20] is a cornerstone of democracy. This guarantee includes the right to hold opinions without interference and the right to receive and impart information. Any limitations placed on this right must meet the standards required and justified by provisions in Article 19(3)

[16] The coalition had its sixth meeting in Costa Rica in October 2016. For more information, please visit:

[17] For more information on the Internet Governance Forum, please visit: https://www.intgovforum.org/multilingual

[18] For more information, please visit:

[19] Examples include the 'Coalition Submission to the Universal Periodic Review of India - Internet Rights, Freedom of Expression (FOE) Online and Freedom of Association and Assembly (FOAA) Online in India' by Digital Empowerment Foundation, Internet Democracy Project, Point of View, Nazdeek and Association for Progressive Communications ( and the (https://www.apc.org/en/pubs/joint-submission-internet-related-human-rights-iss-1).

[20] Guaranteed by Article 19 of the Universal Declaration of Human Rights as well as the International Covenant on Civil and Political Rights.

of the International Covenant on Civil and Political Rights (ICCPR) and must not put in jeopardy the right itself.[21]

General Comment No. 34 issued by the UN Human Rights Committee is an authoritative interpretation of the minimum standards guaranteed by Article 19 of the ICCPR. It states that Article 19 protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression.[22] Therefore, the right to freedom of expression was not designed to fit any particular medium or technology. Regardless of whether it is exercised online or offline, it is an internationally protected right to which almost all countries of the world have committed themselves (ARTICLE 19, 2013).

Across Southeast Asia individuals have been charged, arrested and intimidated for their expression online. The risks of this happening are particularly heightened when expression touches upon political issues or human rights defence. Violations take the form of censorship, surveillance, network disruptions, blocking of websites and webpages, takedown of content, criminalisation and imposition of greater punishments for expression online (Association for Progressive Communications *et al*., 2016). When subjected to these violations, people often self-censor, and as a result their ability to form an opinion may be restricted, as they cannot freely search for and disseminate information or opinions online.

### *Freedom of religion or belief*

Freedom of religion or belief,[23] which includes theistic, non-theistic and atheistic beliefs, as well as the right not to profess any religion or belief,[24] is also largely impacted by the internet. Increasingly, individuals are relying on the internet to seek and impart information about religions and faiths as well as points of view about them. Online spaces also provide a new platform where

[21] As per HRC General Comment No. 10: Article 19 (Freedom of expression), 29 June 1983, available at . An additional requirement is provided in Article 20 of the ICCPR, which declares that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

[22] General Comment No 34, CCPR/C/GC/3.

[23] Guaranteed by Article 18 of the ICCPR.

[24] As per HRC General Comment 22: Article 18 (Freedom of Thought, Conscience or Religion), 30 July 1993, available at:

individuals can express their opinions or views about religions and seek answers to questions they may have. However, this space available for expressing opinions in relation to religion has consistently come under attack, especially in online spaces (Khandhadai, 2016).

Expression relating to religion in online spaces has been increasingly met with censorship and criminalisation and has, at times, resulted in offline attacks and killings in Asia (*Ibid*.). A serious issue in this regard is the growing discourse in support of applying blasphemy laws to online content. Despite repeated calls by international experts and groups to decriminalise and repeal blasphemy-related laws,[25] these laws are being used to combat dissent and criticism of religions or beliefs, which is proving to be a serious threat to the fundamental exercise of freedom of expression online as well as the right to freedom of religion or belief. Laws that punish blasphemy or 'hurting religious sentiments' have a stifling effect on dissent and freedom of expression, prohibiting a free exchange of ideas and views on political, social, legal and academic issues that may touch upon religion (Association for Progressive Communications *et al*., 2017a).

### *Privacy*

The right to privacy[26] embodies the concept that individuals have the right to determine who has information about them and to control how, when and to what extent that information is communicated. The right to privacy is a fundamental human right. It is an important safeguard of individual autonomy and human dignity, as it allows individuals to make choices about how they live their lives. It is essential to the exercise and enjoyment of other fundamental human rights, particularly those related to freedom of expression and belief (Nyst, 2013).

---

[25] See, for example, the Jakarta Recommendations on Freedom of Expression in the Context of Religion, available at ; HRC General Comment No. 34: Article 19 (Freedom of Opinion and Expression), available at ; Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence - Conclusions and recommendations emanating from the four regional expert workshops organised by OHCHR, in 2011, and adopted by experts in Rabat, Morocco on 5 October 2012, available at ; and Report of the Special Rapporteur to the General Assembly on hate speech and incitement to hatred, , available at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx.

[26] Guaranteed by Article 12 of the United Nations Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

In the digital age there are several daunting challenges to the right to privacy.[27] The UN General Assembly and Human Rights Council have recognised these challenges and have called upon states to uphold the right to privacy in digital spaces.[28] Surveillance is a serious and growing challenge to privacy. At a time when massive amounts of data are collected about individuals, states are conducting unlawful and/or arbitrary surveillance, interception of communications, and collection of personal data, which are highly intrusive acts that violate the right to privacy and can interfere with other human rights, like the right to freedom of expression. In particular, mass surveillance fails to meet the tests of necessity and proportionality and may undermine the tenets of a democratic society. Both communications surveillance – including surveillance of online activity and interception of telephone communications – and physical surveillance are popular means of countering crime, disorder and terrorism, as well as pursuing other national security aims. However, these legitimate aims are often used as justification for disproportionate measures, like mass surveillance, and can be abused for more pernicious means, like cracking down on human rights defenders, journalists, and others who challenge the power dynamics within society.

Another of the chief challenges to privacy is data protection or the protection of personal data and information. Identification systems, including ID cards and biometric and DNA databases, are increasingly being adopted by governments as a means of keeping track of citizens and improving the delivery of public services, increasing the effectiveness of law enforcement efforts, and managing migration. ID systems challenge the right to privacy in that they involve the collation and aggregation of large amounts of information that subsequently becomes representative of an individual, without any guarantee of the veracity of that information.

### *Freedom of assembly and association*

Freedom of assembly and association[29] online refers to peoples' use of ICTs to exercise their rights to peacefully assemble or associate, either offline or online. Civil society, human rights defenders,

---

[27] For an overview by the UN Office of the High Commissioner for Human Rights on the Right to Privacy in the Digital Age, please visit: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

[28] See, for example, United Nations General Assembly resolution A/C.3/71/L.39/Rev.1, available at https://www.accessnow.org/cms/assets/uploads/2016/09/privacy-resolution-2016-UNGA.pdf

[29] Guaranteed in Article 20 of the UDHR and Articles 21 (peaceful assembly) and 22 (association) of the ICCPR.

youth, marginalised groups and political parties use ICTs for social and political causes (Comninos, 2012). Tools like websites, email groups, mailing lists and social media platforms are used to share information, organise protests or issue joint statements. There are many examples of like-minded citizens rallying for a cause or coming together informally, whether in a geographical location or across borders, utilising growing access to the internet (Venkiteswaran, 2016). For some, the internet offers possibilities to come together with relative safety, where physical gatherings are dangerous. Often, offline and online platforms are used in combination to complement each other.

However, the internet has also made it possible for non-democratic forces, including state and non-state actors, to occupy the spaces at the same time. In some cases, the aim is to disrupt online social movements or to target individuals for their identities and beliefs. Political parties and religious groups are among the major users of the internet to mobilise supporters and in the process, dominate the online public sphere, and as a result offline threats have been replicated and intensified in online spaces (*Ibid*.).

### *Gender, discrimination and violence*

The internet is a critical space for women and sexually marginalised groups to explore issues related to identity, and access information related to sexual orientation and gender identity (SOGI), including on health and education (Kaye, 2015; Association for Progressive Communications *et al*., 2015). This is especially critical for sections of society who already face extensive regulation, silencing and discrimination on the basis of their sexuality and gender. Yet governments in the region censor SOGI-related online content deemed to offend religious and moral sentiments. In some cases civil society advocating for these rights have been targeted (Mageswari, 2016), and in other cases online content relating to sexual rights has been censored (Jakarta Post, 2016).

Violence against women and girls online – such as cyberstalking, cyberbullying, harassment and misogynist speech – limits their ability to take advantage of the opportunities that ICTs provide for the full realisation of women's human rights. Just as violence is used to silence, control and keep women out of public spaces offline, women’s and girls' experiences online reflect the same pattern. Online violence includes attacks on their sexuality, exposure of personal information, and, in the digital age, the manipulation of images that are then used for blackmail and destroying their

credibility. The consequence of this is that women and girls self-censor, reduce their participation or withdraw from platforms and technology they are using all together. In addition, the normalisation of violent behaviour and the culture that tolerates the violence against women which social media perpetuates and facilitates at rapid speed work to reinforce sexist and violent attitudes, and contribute to norms and behaviour that make online spaces hostile towards women.

In addition, gender-based hate speech online in the name of religion remains largely unaddressed, and women and people who face discrimination based on their sexual orientation or gender identity face severe persecution online, frequently putting them at risk of physical attack as well (Council of Europe, 2016).

### *Economic, social and cultural rights*

Civil and political rights as they pertain to the internet have received much more global attention compared to economic, social and cultural rights (ESCRs). While there have been significant efforts to use the internet to enable access to education, health and food security among other ESCRs, these initiatives have rarely been framed in terms of rights discourse (Brown & Finlay, 2016). The International Covenant on Economic, Social and Cultural Rights (ICESCR) consists of 31 articles dealing with rights such as the right to education,[30] to take part in cultural life and enjoy the benefits of scientific progress and its applications,[31] to work,[32] to health[33] and to food.[34] The internet can impact positively on most articles in the ICESCR. For example, it helps people find work, and unions to organise; it enables small farmers to access competitive market information; it is a powerful enabler of cultural participation, innovation and artistic expression; it allows online learning resources to be shared easily; and it facilitates access to information on health and medical advice.

[30] Guaranteed by Article 13 of the ICESCR.

[31] Guaranteed by Article 15 of the ICESCR.

[32] Guaranteed by Article 6 of the ICESCR.

[33] Guaranteed by Article 12 of the ICESCR.

[34] Guaranteed by Article 11 of the ICESCR.

However, the internet and new technologies can also act as disablers of ESCRs, or even facilitate the violation of rights, as those who are denied access to ICTs are also those who are traditionally marginalised economically and socially. Lack of access further marginalises these groups and alienates them from the process of development at a personal and national level.

More examination is needed on the impact of the internet and ICTs on the exercise of ESCRs at the national level, which is something NHRIs could contribute to.

***Laws regulating the internet***

States, realising the empowering impact of the internet, have in some cases tried to impose greater regulation. Offline regulations, typically in penal legislation, are being applied to online spaces, to bolster internet-specific legislation (Association for Progressive Communications *et al*., 2016). Legitimate expression and exercise of rights on the internet are, as a result, increasingly being redefined as cybercrime.

The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (2011: 10), stated in his 2011 report:

> Legitimate 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.

To take some examples from Southeast Asia, states such as Thailand (Amnesty International, 2016; Human Rights Watch, 2016) and Myanmar are imposing more severe punishments and penalties for expression online than for expression offline. In countries like Malaysia (Association for Progressive Communications, 2016), and Cambodia (Cambodian Center for Human Rights, 2013), new legislation or amendments are currently being formulated which are likely to further restrict the environment for free expression. The institutionalisation of such restrictions, in

contravention of international law,[35] guarantees and obligations, has made it very difficult for human rights defenders and civil society to advocate for reforms and to defend free expression.

Legitimate expression online is often prosecuted as blasphemy, obscenity, sexual deviance, sedition, and criminal defamation. States often rely on public order, national security and religion-based exemptions to crack down on legitimate forms of expression and dissent. Non-state actors, some of whom benefit from the tacit support of the state, have attacked (and sometimes killed) individuals for expressing themselves online (Association for Progressive Communications *et al*., 2017b).

NHRIs play a key role in addressing rights violations in online spaces and in ensuring that laws and regulations seeking to govern the internet have a human rights-based approach and do not legitimise violations.

## 5. Recommendations

### *Digital tools*

NHRIs can:

- Explore and utilise ICTs including email, video conferencing and chat applications to improve efficiency in the way they function and carry out their mandate.
- Develop practices that help them systematically record and store information about their work in digital form.
- Ensure that their websites are accessible and updated and that they carry the information necessary for people to understand their rights and the function of the NHRI.
- Ensure that their websites are compliant with World Wide Web Consortium (W3C) accessibility standards.

[35] As per HRC General Comment No. 34: Article 19 (Freedom of Opinion and Expression), available at

- Proactively disclose all information, unless there is a specific reason to withhold it (for example, the privacy of victims), in line with principles of freedom of information.
- Enable submission of complaints through their websites and ensure that the process for filing these complaints is accessible to different users.
- Establish and maintain a strong presence in social media as a means of monitoring human rights violations through and on this medium and communicating with victims and the public in general.
- Collect data ethically and use the data aggregated through the website in the annual and periodic reports.

***Digital security***

NHRIs can:

- Integrate digital security as a component of a larger integrated security policy and measures.
- Determine what data they need to protect in their investigation of human rights violations, and whom they need to protect it from in order to keep it secure from unauthorised access and abuse.
- Based on the assessment of what data they must protect, develop or adopt a holistic internet and communication policy that helps the institution stay effective and secure.
- Work with experts in the field of data protection and security to put in place measures, processes and tools that help them protect and secure this data.
- Use online communication services with an encryption protocol to avoid unlawful interception of communications.
- Prevent others from having access to visitors' or NHRI website users' sensitive information as it passes through the internet, by enabling HTTPS (a communications protocol for secure communication over a computer network) on their websites.

- Save encrypted backups of their documentation and store it in devices and services that enable robust security features, including encryption.

***Human rights online***

*Internet rights promotion*

NHRIs can:

- Recognise, reinforce and remind stakeholders that human rights offline are applicable to online spaces as well.
- Contribute to the creation of a national culture of respect for human rights on the internet by acknowledging the role that ICTs play in the exercise and advancement of human rights.
- Increase public awareness of human rights online through campaigns, seminars, press conferences, etc., similar to the initiatives currently undertaken in relation to human rights addressed by the NHRIs.
- Work closely with governments and other authorities to ensure that they adopt a human rights-respecting approach to internet and digitalisation initiatives.
- Play a crucial role in the development, formulation and delivery of education initiatives that explain the integral role ICTs play in the exercise and advancement of human rights.
- Impart trainings about human rights online for key groups such as NGOs, judges, police, journalists, etc., to raise awareness about ICT policies and help ensure a human rights-based approach to ICT laws and policies.

*Internet rights protection*

NHRIs can:

- Investigate human rights abuses and violations that take place whether in part or wholly on the internet.

- Work in collaboration with national experts from civil society, academia and the technology sector to address the impact of ICT policies on human rights.
- Monitor and comment on legislation and policies that can undermine the exercise of human rights on the internet.
- Advocate for a human rights-based approach to legislation and policies that seek to govern and regulate online spaces.
- Include reports on human rights on the internet in the UPR process and other human rights monitoring bodies.

**References**

Amnesty International (2016) ‘Thailand: Grave concern over Thai Computer Crimes Act’, 7 October, at: https://www.amnesty.org/en/documents/asa39/4944/2016/en

ARTICLE 19 (2013) *Freedom of expression and ICTs: Overview of international standards*

ASEAN (2015) *The ASEAN ICT Masterplan 2020*, at: http://www.mptc.gov.kh/files/2016/03/499/1.pdf

Association for Progressive Communications (2011) *Closer Than Ever: A guide for social change organisations who want to start working online*, at: https://www.apc.org/en/node/12590

Association for Progressive Communications, International Gay and Lesbian Human Rights Commission and International Lesbian and Gay Association (2015) ‘Joint statement at the interactive dialogue with the Special Rapporteur on freedom of opinion and expression, 29th session of the Human Rights Council’

Association for Progressive Communications (2016) ‘Malaysian parliament should heed civil society calls to reject flawed Communications and Multimedia Act amendments’, at: https://www.apc.org/en/pubs/malaysian-parliament-should-heed-civil-society-cal

Association for Progressive Communications, Bytes for All, Pakistan, Digital Empowerment Foundation and Persatuan Kesedaran Komuniti Selangor (EMPOWER) (2016) ‘Joint written statement submitted to the 32nd session of the Human Rights Council: State of Internet Rights in India, Malaysia and Pakistan’, at: https://www.apc.org/sites/default/files/IMPACT_Written_statement_HRC32_1.pdf

Association for Progressive Communications, Bytes for All, Pakistan, Digital Empowerment Foundation and Persatuan Kesedaran Komuniti Selangor (EMPOWER) (2017a) 'Joint written statement submitted by the Association for Progressive Communications to the 34th session of the Human Rights Council: Freedom of expression and religion in Asia', at: https://www.apc.org/en/node/22510

Association for Progressive Communications, Bytes for All, Pakistan, Digital Asia Hub, Digital Empowerment Foundation, Internet Democracy Project, Persatuan Kesedaran Komuniti Selangor (EMPOWER) and Southeast Asian Press Alliance (2017b) 'Joint written statement submitted by the Association for Progressive Communications to the 35th session of the Human Rights Council: Criminalisation of Online Expression in Asia', at: https://www.apc.org/en/node/33972

Brown, Deborah and Alan Finlay (2016) 'Key considerations: Economic, social and cultural rights and the internet', in A. Finlay (ed.), *Global Information Society Watch 2016*, at: http://www.giswatch.org/en/economic-social-and-cultural-rights-escrs/key-considerations-economic-social-and-cultural-rights-

Brown, Deborah and Sheetal Kumar (2016), *Using the Universal Periodic Review for Human Rights Online*, London: Global Partners Digital, at: https://www.apc.org/sites/default/files/UPR%20Brief%2001072016_1.pdf

Cambodian Center for Human Rights (2013) 'Freedom of Expression and Internet Censorship in Cambodia', at: http://cchrcambodia.org/index_old.php?url=media/media.php&p=analysis_detail.php&anid=34&id=5

Comninos, Alex (2012) *Freedom of Peaceful Assembly and Freedom of Association and the Internet*, Johannesburg: Association for Progressive Communications, at: www.apc.org/en/pubs/freedom-peaceful-assembly-and-freedom-association

Council of Europe (2016) *Combating Sexist Hate Speech*, at: https://rm.coe.int/1680651592

Esterhuysen, Anriette (2016) 'Why focus on economic, social and cultural rights? Reflections on trends, achievements and challenges in building a global movement working for human rights on the internet', in A. Finlay (ed.), *Global Information Society Watch 2016*, at: http://www.giswatch.org/en/report-introduction/why-focus-economic-social-and-cultural-rights-reflections-trends-achievements

Human Rights Watch (2016) 'Thailand: Cyber Crime Act Tightens Internet Control', 21 December, at: https://www.hrw.org/news/2016/12/21/thailand-cyber-crime-act-tightens-internet-control

Jakarta Post (2016) 'Government drafts ban on LGBT websites', 5 March, at:

Kaye, David (2015) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', 22 May, A/HRC/29/32, at:

Khandhadai, Gayatri (2016) *Desecrating Expression: An Account of Freedom of Expression and Religion in Asia*, Bytes for All and FORUM-ASIA, at: https://www.forum-asia.org/uploads/wp/2016/12/Final_FoER_Report.pdf

La Rue, Frank (2011) ‘Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion’, 16 May, A/HRC/17/27, at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

Mason, Stephen (2016) *The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof - a comparative study and analysis*, Strasbourg: European Committee on Legal Co-operation, at: https://rm.coe.int/1680700298

Mageswari, M. (2016) ‘SIS’ application for judicial review dismissed’, *The Star Online*, 25 June, at: http://www.thestar.com.my/news/nation/2016/06/25/sis-application-for-judicial-review-dismissed

Nyst, Carly (2013) ‘Internet Rights Are Human Rights: The right to privacy’, at: http://itrainonline.org/itrainonline/mmtk/APC_IRHRCurriculum_Privacy_Handout.pdf

Souter, David (2013) ‘Introduction to Human rights, ICTs and the internet’, at: http://itrainonline.org/itrainonline/mmtk/APC_IRHRCurriculum_Intro_Handout.pdf

Venkiteswaran, Gayathry (2016) *Freedom of assembly and association online in India, Malaysia and Pakistan: Trends, challenges and recommendations*, Montevideo: Association for Progressive Communications, at: www.apc.org/en/system/files/FOAA_online_IndiaMalaysiaPakistan.pdf