6

International human rights law

1. It is widely accepted that many of the international human rights that individuals enjoy 'offline' are also protected 'online'.[389] This Chapter articulates Rules indicating the scope of application and content of international human rights law bearing on cyber activities. Although the International Group of Experts agreed that both treaty and customary international human rights law apply to cyber-related activities, they cautioned that it is often unclear as to whether certain human rights reflected in treaty law have crystallised as rules of customary law. Moreover, aspects of international human rights treaty law are subject to variance when States and regional bodies interpret them *vis-à-vis* cyber activities. The Experts further noted that States may, under specific circumstances (Rule 37), limit the exercise and enjoyment of certain rights in accordance with international human rights law.

2. The Universal Declaration of Human Rights is often cited as reflective of certain key customary norms.[390] Many provisions of international human rights treaty law, including certain of those found in the

[389] *See, e.g.*, The Promotion, Protection and Enjoyment of Human Rights on the Internet, para. 1, UN Doc. A/HRC/32/L.20 (27 June 2016); The Right to Privacy in the Digital Age, GA Res. 68/167, para. 3, UN Doc. A/RES/68/167 (18 December 2013); EU Human Rights Guidelines on Freedom of Expression Online and Offline, Council of the European Union, para. 6 (12 May 2014); UN GGE 2013 Report, para. 21; UN GGE 2015 Report, paras. 13(e), 26; NATO 2016 Warsaw Summit Communiqué, para. 70; Convention on Cybercrime, pmbl., Art. 15.1; Deauville G8 Declaration: Renewed Commitment for Freedom and Democracy, para. II(10) (26–27 May 2011); Agreement between the Governments of the Member States of Shanghai Cooperation Organization on Cooperation in the field of International Information Security, Art. 4(1), 16 June 2009.

[390] UN International Conference on Human Rights, Final Outcome Document, para. 2, UN Doc. A/CONF.32/41 (13 May 1968). ('[T]he Universal Declaration of Human Rights . . . constitutes an obligation for the members of the international community'.). For an example of one State's view as to those international human rights law norms that are customary in nature, see Restatement (Third), Sec. 702.

ICCPR and the ICESCR, are also regarded as reflective of customary international law. However, no definitive catalogue of customary international human rights law exists. Additionally, not all States are Parties to the same international human rights law treaties and the rights accorded to individuals under regional human rights instruments, and the scope of those rights, vary. Even within regional systems, there is often a margin of appreciation that reflects respect for differences in, *inter alia*, capacity and national legal tradition. Finally, some treaties allow States to issue reservations to their provisions when they become Parties thereto or subsequently derogate (Rule 38) from their obligations under the treaty in exceptional circumstances provided for in the instrument.

3. This Chapter relies heavily upon various human rights treaties, as well as case law interpreting and applying them. Such instruments are directly binding only on Parties thereto and it is inappropriate to freely generalise from one treaty regime to another. Nevertheless, the Experts agree that treaty provisions shed light, in a general sense, on the scope of applicability and content of corresponding customary international human rights norms. In particular, whenever multiple treaties and case law adopt the same or a similar position regarding a particular human right, the International Group of Experts agreed that such congruence may support, but does not necessarily do so definitively, a conclusion that customary international law exists to that effect. Accordingly, the Experts took a conservative approach in drafting the Rules that follow.

4. Although the Experts concluded the Rules set forth in this Chapter are meant to apply globally, they also agreed with the assertion that 'the realisation of human rights must be considered in the regional and national context bearing in mind different political, economic, legal, social, cultural, historical and religious backgrounds'.[391] This point is especially relevant in the cyber context given differing levels of cyber development, economic wherewithal, national and regional security concerns, and the like. However, the Experts concurred that such factors do not relieve States of their customary human rights law obligations, except in accordance with the limitations set forth in Rule 37 or a treaty provision permitting derogation (Rule 38). Rather, these factors are to be considered when assessing how the right in question applies to a

[391] ASEAN Human Rights Declaration, Art. 7.

situation, as well as the nature of the limitations, if any, that a State may impose on its exercise or enjoyment.

5. The International Group of Experts was in accord that States must not only respect human rights, but also protect (i.e., ensure respect for) them. The obligation to respect denotes a duty to refrain from unlawfully interfering with human rights that individuals enjoy. In other words, it applies with regard to the activities of a State *vis-à-vis* each individual enjoying the human right in question. By contrast, the obligation to protect refers to the legal requirement to take measures to ensure third parties do not interfere with the enjoyment of human rights. The parameters of these two obligations, and limitations thereon, are dealt with in Rule 36.

6. The precise interplay between the law of armed conflict (Part IV) and international human rights law remains unsettled and is determined with respect to the specific legal rules in question. Nevertheless, the International Group of Experts was unanimous in the view that both the law of armed conflict and international human rights law apply to cyber-related activities in the context of an armed conflict, subject to the application of the principle of *lex specialis*.[392] For instance, although human rights treaty provisions prohibiting arbitrary deprivation of life are non-derogable,[393] whether a cyber attack (Rule 92) during an armed conflict violates that prohibition is determined primarily by reference to the *lex specialis* law of armed conflict rules regarding the conduct of hostilities (Chapter 17).

7. Rule 34 affirms the general premise that individuals enjoy customary international human rights law protections with respect to their cyber-related activities. The following Rule examines some of the key international human rights that individuals enjoy with respect to such cyber-related activities. It must be cautioned that although a State's activity may interfere with a specific international human right, such as the right to privacy, this fact does not answer the question of whether that right has been violated. Violation is a separate issue. In this regard, human rights law

[392] *Nuclear Weapons* advisory opinion, para. 25; *Wall* advisory opinion, paras. 106, 142. *See also* General Comment No. 31, para. 11. Some of the Experts emphasised that *lex specialis* is not to be understood as only a matter of the law of armed conflict overriding international human rights law. Rather, *lex specialis* is a means of interpretation and conflict resolution in the event a specific rule within one legal regime conflicts with a rule from another; it is but part of a system of legal methodology and interpretation.

[393] *See, e.g.*, ICCPR, Arts. 4(2), 6(1); ACHR, Arts. 4, 27(2); African Charter, Art. 4; ECHR, Arts. 2, 15(2).

obligations, with the exception of absolute rights, are subject to limitation by the State in certain circumstances. Furthermore, most human rights treaties allow for States to derogate from some of their obligations, albeit only to the extent delineated by those instruments and in accordance with international law. This means that a State has only violated international human rights law if (1) it owes international human rights law obligations to the person in question (Rule 34); (2) the person's cyber-related activity falls within the scope of a particular international human right (Rule 35); (3) the State engages in an act that interferes with the international human right in question; and (4) the State has not imposed lawful limitations (Rule 37) on, or derogated from (Rule 38), the right in question.

Rule 34 – Applicability

International human rights law is applicable to cyber-related activities.

1. The International Group of Experts agreed that international human rights law, whether found in customary or treaty law, applies in relation to cyber-related activities. As noted in the chapeau to this chapter, the principle that the same rights people have offline are to be protected online has been asserted repeatedly in numerous multilateral and multi-stakeholder fora. Indeed, at the time international human rights law norms emerged it was recognised, for example, that the right to freedom of expression (Rule 35) extended to 'any' media, a reference that accommodates technological advancements, such as the emergence of cyber-enabled expression.[394] However, the International Group of Experts acknowledged that State understandings concerning the precise scope of certain human rights entitlements in the cyber context, as well as those of human rights tribunals and other relevant human rights bodies, vary.

2. States bear responsibility for international human rights law violations that they themselves commit (*lit.* (a) of Rule 36).[395] Additionally, if the activities of a non-State actor or another State interfere with the ability of individuals to engage in cyber activities protected by international human rights law, States may shoulder an obligation to ensure that the individuals entitled to benefit from the rights in question can do so (*lit.* (b) of Rule 36).

[394] UDHR, Art. 19. *See also* ICCPR, Art. 19(2); ECHR, Art. 10(1); ACHR, Art. 13(1).
[395] *See, e.g.*, *Genocide* judgment, paras. 207–208.

3. The Experts noted that the issue of whether entities other than States are bound by international human rights law and, if so, the extent to which they are so bound, is unsettled and controversial. However, they agreed that international organisations, as legal persons, may be bound by customary international human rights law.[396]

4. The International Group of Experts was of the view that although certain human rights regimes, such as that of the Council of Europe,[397] afford various human rights to legal persons, customary international human rights attach only to natural persons.[398] For instance, if a hostile cyber operation is directed against the website of a human rights organisation, the customary law human rights potentially implicated are those of the organisation's members, not the organisation itself.[399]

5. With regard to the applicability of customary international human rights law, the International Group of Experts concurred that such law applies to all persons on a State's territory irrespective of where the State's cyber activities that implicate the human right in question occur.[400] For instance, a State's human rights law obligations attach when the communications of an individual who is located in its territory are

[396] *See, e.g.*, United Nations Safety Convention, Art. 20(a); Optional Protocol to the United Nations Safety Convention, Art. II(1); Decision No. 2005/24 of the Secretary-General's Policy Committee on Human Rights in Integrated Missions (2005); Capstone Doctrine, at 14–15, 27.

[397] For instance, the European Court of Human Rights has held that the freedom of expression in Art. 10 of the ECHR applies to commercial entities. *See, e.g.*, *Autronic AG* v. *Switzerland*, 12 EHRR 485 para. 47 (2 May 1990).

[398] *See, e.g.*, Human Rights Council, Implementation of General Assembly Resolution 60/251 of 15 March 2006 Entitled 'Human Rights Council': Report of the Special Representative of the Secretary-General (SRSG) on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, para. 38, UN Doc. A/HRC/4/035 (9 February 2007).

[399] The Inter-American Court has afforded legal persons a margin of protection when they are the mechanisms through which natural persons enjoy their human rights. In *Granier and others (Radio Caracas Televisión)* v. *Venezuela*, a television channel received a degree of protection because it was a mechanism by which its owners exercised their right to freedom of expression. Such a holding is especially relevant in the cyber context as companies that operate online are frequently used as a mechanism by which the right is exercised. Case of *Granier and others (Radio Caracas Televisión)* v. *Venezuela*, Judgment, Inter-Am. C.H.R., para. 22 (22 June 2015).

[400] *See, e.g.,* ICCPR, Art. 2(1); ECHR, Art. 1; ACHR, Art. 1(1) (note that the jurisdictional clauses in these instruments differ to a degree with respect to scope of application). *See also* General Comment No. 31, para. 10; *López Burgos* v. *Uruguay*, para. 12.3, UN Doc. Supp. No. 40 (A/36/40) (29 July 1981).

intercepted abroad by that State or when the State acquires access to the individual's data that is stored electronically beyond its borders.

6. The Experts agreed that, as a general principle, customary international human rights law applies in the cyber context beyond a State's territory in situations in which that State exercises 'power or effective control', as it does offline.[401] Power or control may be over territory (spatial model)[402] or over individuals (personal model). A State may be, for example, in effective control of foreign territory (that is, the territory is under the authority of the hostile army) during a belligerent occupation (chapeau to Chapter 19), whether that occupation be lawful or unlawful,[403] or if it leases territory from another State and is granted the right of exclusive control over that territory. With regard to application of the personal model, the Experts agreed that individuals abroad who are physically in the power or effective control of the State, as with those detained by the State, are entitled to have their human rights respected by the State concerned.[404] However, in this latter situation, it may be that only those specific rights relevant to the situation will be engaged.[405]

7. The International Group of Experts acknowledged a viewpoint by which customary international human rights law does not apply at all beyond a State's borders, irrespective of whether the State is exercising power or effective control, but disagreed with that position. The Experts also acknowledged that a number of States accepting the

[401] The term 'power or effective control' is drawn from General Comment No. 31, para. 10. The same concept is expressed somewhat differently in different human rights regimes. For instance, with regard to interpretation of the ECHR in this context, see *Al-Skeini* judgment, paras. 130–139; *Catan* v. *Moldova and Russia*, judgment, App. Nos. 43370/04, 8252/05, and 18454/06, ECtHR, para. 105 (2012).

[402] With respect to the ICCPR, see General Comment No. 31, paras. 3, 10. As to the ECHR, see *Loizidou* v. *Turkey*, App. No. 15318/89, preliminary objections, 310 ECtHR., paras. 61–62 (ser. A) (1995). On the American Declaration of the Rights and Duties of Man, see *Armando Alejandre Jr. et al.* v. *Cuba*, Case 11.589, Rep. No. 109/99, para. 23 (1999).

[403] *See Wall* advisory opinion, para. 109; *Armed Activities* judgment, para. 173. The International Group of Experts noted recent case law of the European Court of Human Rights that emphasises the importance of *de facto* control and notes that not all instances of occupation entail sufficient control for the ECHR rights to apply *in toto*. *Al-Skeini* judgment, para. 139.

[404] *See, e.g., Delia Saldias de López* v. *Uruguay*, Human Rights Committee, Comm. No. 52/1979, para. 12, UN Doc. CCPR/C/OP/1 (1984); *Ocalan* v. *Turkey*, App. No. 46221/99, ECtHR, para. 91 (2005); *Isaak and others* v. *Turkey*, App. No. 44587/98, ECtHR, para. 115 (2006).

[405] *Al-Skeini* judgment, para. 137.

extraterritoriality of customary international human rights law disagree with application of the 'power or effective control' standard. For these States, the standard is limited to specific treaty law. As an example, it applies under the ECHR, but not all States are Parties to the instrument. In the view of these States, it is inappropriate to extend the notion beyond the specific treaties and in the context in which it applies.

8. The International Group of Experts could achieve no consensus as to whether State measures that do not involve an exercise of physical control may qualify as 'power or effective control' in the sense of this Rule. In particular, no consensus could be reached as to whether State activities conducted through cyberspace can give rise, as a matter of law, to power or effective control over an individual located abroad, thereby triggering the extraterritorial applicability of that State's international human rights law obligations.

9. On this issue, the Experts were split. The majority was of the view that, in the current state of the law, physical control over territory or the individual is required before human rights law obligations are triggered.[406] These Experts asserted that the premise of exercising power or effective control by virtual means such that human rights obligations attach runs contrary to both extensive State practice and the paucity of expressions of *opinio juris* thereon. As an example, there is little evidence that when States conduct signals intelligence programmes directed at foreigners on foreign territory, they consider that their activities implicate the international human right to privacy (Rule 35).

10. A few of the Experts took the position that so long as the exercise or enjoyment of a human right in question by the individual concerned is within the power or effective control of a State, that State has power or effective control over the individual with respect to the right concerned. In other words, if an individual cannot exercise a human right or enjoy the protection of one because of a State's action, international human rights law applies extraterritorially. As an illustration of this view, consider the case of a State that interferes with the ability of an individual located abroad to engage in electronic communications, for instance by hacking into the person's email account and changing its password such that the individual no longer

[406] *Al-Skeini* judgment, para. 136.

has access to the account. Because the State's cyber operation restricts the individual's ability to exercise the right to freedom of expression (Rule 35), the State is in power or effective control of the individual with respect to the freedom of expression (but not, for instance, with respect to the right to liberty of movement[407]). Note, however, that this only means that the rights are implicated; whether they have been violated is a separate determination.

11. All of the Experts also agreed that international human rights law treaty provisions setting forth the scope of the applicability of the instrument in question govern the issue of extraterritorial application. For example, there is some disagreement over whether the ICCPR applies extraterritorially.[408] The issue is whether Article 2(1)'s scope provision, which extends protection to 'individuals within its territory and subject to its jurisdiction', is meant to extend the Covenant's obligations abroad. Irrespective of the existence of differing positions on this question, all of the Experts agreed that, as a scope provision, Article 2(1) governs the treaty's extraterritorial applicability, or lack thereof. This observation is fundamental for those assessing the application of international human rights law in the cyber context because the bulk of such law is found in treaties governing the activities of the Parties thereto and because the precise scope of many aspects of customary international human rights law is unclear.

12. The International Group of Experts was split on the issue of whether an international human rights treaty that does not address the issue of extraterritoriality should be interpreted as applying extraterritorially or as limited to the territories of the States Parties to the instrument. Some of the Experts were of the view that unless a treaty so provides, the provisions thereof do not apply extraterritorially. They took the position on the basis that treaty provisions should not be interpreted so as to impose obligations on Parties to which they did not expressly agree. The others would apply the treaty provisions extraterritorially unless the treaty provides otherwise. This approach, in their opinion, better reflects the underlying object and purpose of international human rights law.

[407] ICCPR, Art. 12(1).

[408] *See, e.g.*, UN Human Rights Committee, Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Third Periodic Reports of States Parties, United States of America, para. 3, UN Doc. CCPR/C/USA/3, Annex I (28 November 2005); *Wall* advisory opinion, paras. 109–111.

13. For a discussion of extraterritoriality in the context of a State's obligation to protect individuals from violations of their international human rights, see *lit*. (b) of Rule 36.

Rule 35 – Rights enjoyed by individuals

Individuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy.

1. The application of treaty and customary international human rights law to cyber-related activities encompasses civil, political, economic, social, and cultural rights, that is, all international human rights. The commentary that follows examines certain rights that the International Group of Experts found especially relevant in the cyber context.[409] These include the rights to freedom of expression, privacy, freedom of opinion, and due process. The omission of a purported international human right in this commentary is not to be understood as indicating that the Experts concluded it was not customary in nature.

2. Freedom of expression[410] is an international human right often implicated in the cyber context. This is not only because it is a right in itself, but also because an ability to exercise the right is sometimes necessary for the enjoyment of other human rights. The International Group of Experts agreed that the right of freedom of expression is the 'freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'.[411]

3. Consider State cyber operations directed at online forums, chatrooms, social media, and other websites. Such operations are likely to

[409] The International Group of Experts noted that the enumerated rights in this Rule are not exhaustive. For instance, other rights that may be relevant in the cyber context include the right of association and peaceful assembly (UDHR, Art. 20; ICCPR, Arts. 21–22); liberty and security (UDHR, Art. 3; ICCPR, Art. 9); and protection from defamation (UDHR, Art. 12; ICCPR, Art. 17).

[410] UDHR, Art. 19; ICCPR, Art. 19(2); ECHR Art. 10; ACHR, Art. 13; ACHPR, Art. 9. *See also* General Comment No. 34, para. 12; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, paras. 20–22, UN Doc. A/HRC/17/27 (16 May 2011); Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 11, UN Doc. A/HRC/29/32 (22 May 2015); EU Human Rights Guidelines on Freedom of Expression Online and Offline, Council of the European Union, paras. 16, 18 (12 May 2014).

[411] ICCPR, Art. 19(2). *See also* UDHR, Art. 19; General Comment No. 34, para. 11; ECHR, Art. 10(1); ACHR, Art. 13(1); African Charter, Art. 9.

implicate the right of freedom of expression, for instance when the websites targeted are those of bloggers, journalists, or other individuals that disseminate information embarrassing to the State or to powerful individuals therein. If the expression is of a protected nature, States may only conduct the operations if they are designed to enforce lawful limitations (Rule 37) the State has imposed on the freedom of expression. Similarly, a State could block individuals seeking to express themselves from accessing specific IP addresses or domain names, take down websites, employ filtering technologies to deny access to pages containing keywords or other specific content, or obstruct the sending of email, text, and other forms of point-to-point or group communications. These activities infringe upon the right to freedom of expression when not in accordance with Rule 37. It must be noted that such actions might also violate other rights, such as the freedoms of peaceful assembly and association.[412]

4. Although it could achieve no consensus on the precise parameters of the right to freedom of expression, the International Group of Experts noted that restrictions on certain categories of expression, whether offline or online, are subject to particular scrutiny from an international human rights law perspective. Examples of these categories include discussion of government policies, politics, and elections, as well as reporting on human rights, government activities, and corruption in government.[413]

5. Related to freedom of expression is the separate right to freedom of opinion. States must respect the right of individuals to hold opinions without interference.[414] Although the right to hold an opinion and freedom of expression are closely related, the International Group of Experts agreed that there is a distinction between the two. The right to hold an opinion freely is a guarantee so central to the object and purpose of international human rights law that, unlike the freedom of expression, its exercise may not be restricted. State conduct that interferes with the freedom of opinion includes online incitement against protected persons,

[412] UDHR, Art. 20; ICCPR, Arts. 21–22.

[413] Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development, Human Rights Council Res. 12/16, para. 5(p)(i), UN Doc. A/HRC/RES/12/16 (12 October 2009); Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 42, UN Doc. A/HRC/17/27 (16 May 2011). *See also* General Comment No. 34, para. 23.

[414] UDHR, Art. 1; ICCPR, Art. 19(1); ASEAN Human Rights Declaration, Art. 22.

online intimidation, or other forms of harassment conducted on the basis of a person's views, such as political or religious views that are evidenced by membership in a political party or a religious denomination. The Experts noted that once an opinion is expressed, that expression is subject to limitations by the State in accordance with Rule 37.

6. The right to be free from arbitrary interference with one's privacy is of central importance in the cyber context.[415] The International Group of Experts concluded that the right is of a customary international law character,[416] but cautioned that its precise scope is unsettled and that a number of States that accept the existence of the right take the position that it does not extend extraterritorially (Rule 34). The Experts further noted that privacy is not an absolute right and may be subject to limitations, as discussed in Rule 37. They also acknowledged the existence of a view that the right to privacy has not yet crystallised into a customary norm.

7. All of the Experts agreed that the right to privacy encompasses the confidentiality of communications.[417] As a general matter, communications such as email must be 'delivered to the addressee without interception and without being opened or otherwise read'.[418] For instance, an email sent by one individual to another falls within the scope of the right to privacy. That right is implicated if a State accesses the content of the

[415] UDHR, Art. 12; ICCPR, Art. 17; CRC, Art. 16; CRPD, Art. 22; International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, Art. 14, 18 December 1990, 2220 UNTS 39481. *See also* ECHR, Art. 8; ACHR, Art. 11; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Art. 1, 1 October 1985, ETS No. 108; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 23, UN Doc. A/HRC/23/40 (17 April 2013); The Right to Privacy in the Digital Age, para. 14; Council of Europe, Declaration on Freedom of Communication on the Internet, princ. 7 (2003); *R* v. *Spencer*, 2014 SCC 43, para. 62.

[416] *See, e.g.*, G20 Leaders' Communiqué, Antalya Summit, 15–16 November 2015; Council of Europe, Parliamentary Assembly, Resolution 2045, paras. 4, 10 (21 April 2015); ASEAN Human Rights Declaration, Art. 21; The Right to Privacy in the Digital Age, GA Res. 69/166, pmbl., UN Doc. A/RES/69/166 (10 February 2016).

[417] *See, e.g.,* The Right to Privacy in the Digital Age, para. 17; Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, paras. 16–18; *Copeland* v. *United Kingdom*, judgment, App. No. 62617/00, ECtHR, para. 43 (2007). Article 17 of the ICCPR includes the right to be free from arbitrary or unlawful interference with both privacy and correspondence. The International Group of Experts agreed that the latter is an aspect of the right to privacy and therefore did not treat it separately. The Experts also agreed that use of the term communication is more appropriate in the cyber context than correspondence.

[418] General Comment No. 16, para. 8.

communication. In this regard, the Experts agreed that it is irrelevant whether the communication includes sensitive information.[419]

8. Although the International Group of Experts concurred that human inspection of content implicates the right to privacy, it was divided on the applicability of the right to machine inspection by algorithmic analysis. The Experts were of the view that machine inspection of a communication's content undertaken solely for the efficient and secure operation of a network either does not implicate the right to privacy, or implicates it, but is generally justified (Rule 37). Yet, they could reach no agreement on the circumstances that fell between these examples, such as where a machine engages in the inspection of content to filter for terms that will result in subsequent human inspection.

9. The Experts discussed a scenario in which a State merely collects communications without examining them by either human means or machine, or a combination thereof. The majority position was that the right to privacy is not implicated until such time as the State accesses the content of the communications or, as discussed below, processes personal data found in them. A minority of Experts was of the view that the mere collection of communications, even without accessing them, constitutes an interference with the right of privacy; in such cases, whether it constitutes a violation thereof depends on Rules 37 and 38.[420]

10. The International Group of Experts agreed that the right to privacy with respect to the confidentiality of communications is not implicated when a State accesses publicly available website postings, openly accessible social media sites, or other sources that are generally

[419] *See, e.g.*, Court of Justice of the European Union, *Digital Rights Ireland and Seitlinger and Others*, judgment in joined cases C-293/12 and C-594/12, 2014 ECR 238 (8 April 2014), para. 33.

[420] *See, e.g.*, *Leander* v. *Sweden*, judgment, App. no. 9248/81, ECtHR, para. 48 (1987), in which the Court first held that the storing of information alone can constitute an interference with the right to privacy under the ECHR. *See also* The Right to Privacy in the Digital Age, para. 20. The storing of personal data (see discussion below) is also considered to fall within the scope of the right to privacy under European Union legislation because it constitutes the 'processing of personal data'. Therefore, to the extent the communications that a State stores include personal data, the right to privacy is implicated. *See, e.g.,* Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 2(b) (24 October 1995); Regulation (EU) 2016/679 of the European Parliament and of the Council 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, Art. 4(2) (27 April 2016) (in effect as of 25 May 2018).

available to the public. By contrast, the use of social media to communicate or share material among a small closed group, as in Facebook messaging or use of a limited access cloud drive, is more likely to implicate the right of privacy. The Experts could identify no clear threshold at which the right to privacy is implicated on the basis of the accessibility of communications. Factors other than size of the group that has access may be relevant. For example, if the terms of participation in the closed group provide that communications may not be shared with those beyond the group, the right to privacy is more likely to be implicated by a State accessing them.

11. The Experts discussed whether the right to privacy under customary international law with respect to a communication is dependent upon a reasonable expectation of the parties thereto that the content will not be made known to, or seen by, others. Some of them reasoned that absent such an expectation, there is no colourable basis for asserting that a State has violated an individual's privacy. Other Experts suggested that such a standard is unhelpful because in those cases in which an individual knows the State is conducting operations that intrude into his or her communications, for instance because it has been reported on the media that the State engages in particular large-scale surveillance operations, the individual may not logically harbour any expectation that the communications will remain confidential. For these Experts, therefore, imposing such an expectation would be an overbroad exclusion of the right.

12. The International Group of Experts agreed that in addition to the confidentiality of communications, the right to privacy generally protects the personal data of individuals.[421] It acknowledged that the precise definition of 'personal data' is a matter that has generated a degree of controversy with respect to regional human rights regimes and national laws.[422] The Experts were likewise unable to articulate the precise scope of the concept in the more ambiguous environment of customary international law. Nevertheless, certain examples are clear. Information

[421] *See, e.g.,* ASEAN Human Rights Declaration, Art. 21; General Comment No. 16, para. 10; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Art. 1, 1 October 1985, ETS No. 108.

[422] In this regard, personal data is sometimes referred to as personally identifiable information. The Experts noted that in regional human rights regimes the protection of personal data is occasionally treated as a right distinct from that of privacy. For example, the Charter of Fundamental Rights of the European Union provides for the 'right to respect for . . . communications' in Article 7 and 'right to the protection of personal data' in Article 8.

contained in health records or that is submitted to acquire security clearances, for example, is of such a personal nature that it unambiguously qualifies. Whether a State that accesses, copies, or extracts such data relating to individuals located on another State's territory has violated the concerned individuals' international human right to privacy depends on (1) extraterritorial application (Rule 34) of the right, and (2) whether the activity was consistent with the lawful limitations on, and derogations from, that right (Rules 37–38).

13. The Experts considered the issue of whether the collection and processing of metadata by a State is encompassed within the scope of the right to privacy, either as personal data or as a part of a communication. In their view, metadata may constitute personal data if the captured metadata is subsequently linked to an individual and relates to that individual's private life. They suggested, for example, that if a State, based on an individual's web browsing metadata, is able to ascertain aspects of that individual's health or personal relationships, the right to privacy is implicated. In drawing these conclusions, the Experts felt the need to emphasise that State practice and *opinio juris* on this matter are limited.

14. Despite consensus that metadata qualifying as personal data is protected by the right to privacy, the Experts did not reach agreement regarding other types of metadata. A minority of the Experts took the position that all metadata associated with confidential communications constitutes an integral element thereof and is thus protected as a communication.[423] The majority countered that the meaning of the notion of 'communications' that falls within the right to privacy is only to be understood as extending to the content thereof, such as the body of an email, and not the associated metadata. For them, metadata *per se* is not protected as an element of a confidential communication, but, as discussed, may be protected as personal data. To illustrate, metadata indicating the sender and recipient of an email implicates the right to privacy because it is likely to constitute, by this approach, personal data, but metadata that denotes whether a confidential email communication employed an IMAP or POP3 email protocol does not.

15. The Experts noted that States frequently engage in cyber espionage (Rule 32), both within and beyond their territories. Although questions might arise as to the extraterritorial application of international

[423] *See, e.g.*, *Malone* v. *United Kingdom*, App. No. 8691/70, 82 ECtHR (ser. A), para. 84 (1984).

human rights law (Rule 34) with respect to espionage, the Experts were aware of no *opinio juris* suggesting that States consider espionage *per se* to fall beyond the bounds of their international human rights law obligations concerning the right to privacy. As such, the Experts concluded that, notwithstanding State practice, espionage remains subject to States' applicable human rights law obligation to respect the right to privacy.

16. With respect to the right to due process,[424] the International Group of Experts concurred that individuals who are suspected or convicted of committing cyber crimes enjoy the protection of the same international human rights law norms pertaining to law enforcement and judicial processes that are due individuals suspected or convicted of committing non-cyber crimes. The Experts were of the view that there is no justification for a relaxation of the established norms for independent and impartial investigation, due process in relation to any arrest and subsequent pre-trial detention, fair and independent trial procedures, and standards of treatment in post-conviction detention in the case of cyber crime.

17. The Experts took particular note of the increasing importance of electronic sources of evidence in the investigation and prosecution of criminal activity, the seizure of which may raise international human rights issues. For example, if an individual is accused of maliciously hacking into the website of a business, law enforcement officials may want to gain access to some of the individual's data, such as personal electronic communications, to establish guilt. In this regard, the limitations on a State's searches deriving from international human rights law that regulate other types of searches, including the obligation to respect the right to privacy, apply *mutatis mutandis* to remote searches of an individual's networks or online storage. The Experts noted in this regard that States are promulgating domestic laws regarding remote access by cyber means for law enforcement and other purposes.[425] With regard to the lawfulness of a law enforcement agency's unilateral acquisition of electronic evidence from cyber infrastructure located abroad, see Rule 11.

[424] UDHR, Arts. 9–11; ICCPR, Arts. 9–11, 14–15. *See also, e.g., Premininy* v. *Russia*, judgment, App. No. 44973/04, ECtHR, paras. 119–124 (2011).

[425] *See, e.g.*, Search and Surveillance Act 2012, Public Act 2012 No. 24 (5 April 2012), Secs. 111, 114 (N.Z.).

18. As with the aforementioned civil and political rights, the International Group of Experts agreed that the enjoyment of certain economic, social, and cultural rights is increasingly dependent on cyber activities. These rights include, *inter alia*, the right to an adequate standard of living, including adequate food, the right to the enjoyment of the highest attainable standard of physical and mental health, the right to work, the right to education, and the right to take part in cultural life.[426] For instance, the Committee on Economic, Social and Cultural Rights has stated that the enjoyment of the highest attainable standard of physical and mental health includes 'the right to seek, receive and impart information and ideas concerning health issues'.[427] A State's cyber activities that prevent access to valid health information or services on the Internet implicate this right. Online surveillance activities may also implicate the right if, for example, an individual refrains from seeking or communicating sensitive health-related information out of fear that his or her condition may be revealed to others.

19. The Experts noted that the customary status of particular economic, social, and cultural rights is unsettled. Indeed, some States take the position that no such rights are customary in nature and that they are instead exclusively treaty commitments of States that are Parties to the relevant instruments. The Experts also noted that a State's obligations in the realm of these rights, if and to the extent they reflect customary international law, are variable; in particular, they may depend on the resources available to the State.[428]

20. The International Group of Experts discussed whether there is a so-called 'human right to anonymity' *per se* and agreed that international law has not crystallised with respect to a right to be anonymous on the Internet. Therefore, they took the position that although actions to prohibit, restrict, or undermine access to devices

[426] ICESCR, Arts. 6, 11–13, 15; UDHR, Arts. 23, 25(1), 26–27; CERD, Art. 5; CEDAW, Arts. 10–13; CRC, Arts. 2, 17, 23–24, 28–29, 31; European Social Charter, Arts. 1, 11, 21, 29, 3 May 1996, ETS No. 163; African Charter, Arts. 15, 16–17, 22; Additional Protocol to the American Convention on Human Rights, Arts. 6, 10, 12–14, 17 November 1988, OASTS No. 69.

[427] Office of the High Commissioner for Human Rights, CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12), para. 12(b), UN Doc. E/C.12/2000/4 (11 August 2000).

[428] ICESCR, Art. 2(1). *See also* CESR General Comment No. 3: The Nature of State Parties' Obligations (Art. 2(1) of the Covenant), para. 10, UN Doc. E/1991/23 (14 December 1990).

or technology that foster anonymity may, as a practical matter, reduce the exercise or enjoyment of international human rights online, such actions do not in themselves necessarily implicate international human rights law as a matter of *lex lata* on the basis of infringement with or loss of anonymity.

21. That said, the Experts noted that an ability to be anonymous in cyberspace may bear on the exercise of the freedom of expression and the enjoyment of the right to privacy. Consider a situation in which a State requires individuals who post material protected by the right to freedom of expression on the Internet to identify themselves. The requirement effectively deters them from engaging in protected expression and, thus, in the view of the Experts, constitutes an interference with that right. Accordingly, any such requirement would need to be justified pursuant to one of the grounds set forth in Rule 37. The same legal reasoning applies in the case of the right to privacy. For instance, a State may not process metadata to identify participants in an anonymous online survey that collects personal health data unless the processing complies with that Rule.

22. In the view of the International Group of Experts, 'access to the Internet' is also not an international human right in itself as a matter of customary international law; technology is an enabler of rights, not a right as such. Nevertheless, State measures limiting access to or use of the Internet must be consistent with the exercise or enjoyment of international human rights, such as those cited earlier in this commentary. A State that blocks access to the Internet throughout the country during civil disturbances is, for instance, in violation of the right to freedom of expression if the limitations on the exercise of that right caused by the blockage are not in compliance with the criteria set forth in Rule 37.

23. The International Group of Experts further agreed that no customary international human 'right to be forgotten' currently exists. A purported right of individuals to have certain data removed from the Internet has been asserted in litigation.[429] While such litigation may have

[429] For instance, in *Google* v. *Spain*, the Grand Chamber of the Court of Justice of the European Union ruled that Google is a data controller for the purposes of the European Union's Data Retention Directive. As a result, Google was obliged to protect the fundamental rights of the owner of that data, in particular, the 'right to be forgotten', by responding to requests that certain dated data be removed from the Internet. *Google Spain SL, Google Inc.* v. *Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez* (case C-131/12), ECR, 13 May 2014; Judgment of Judge

ramifications for future regulation of search engines and Internet service providers, the Experts were of the view that, at present, there is no customary international human rights law-based obligation of States to require third parties to remove personal data or links to that data from the Internet on the basis of a 'right to be forgotten'.

Rule 36 – Obligations to respect and protect international human rights

With respect to cyber activities, a State must:

(a) respect the international human rights of individuals; and
(b) protect the human rights of individuals from abuse by third parties.

1. International human rights law requires States to respect, as well as to protect (i.e., ensure respect for), human rights.[430] The International Group of Experts agreed that these obligations apply in cyberspace.[431] An obligation to 'fulfil' is not included in this Rule for the reasons set forth below.

2. Pursuant to *lit.* (a), States must refrain from activities that violate the human rights individuals enjoy in cyberspace. Some of the key rights are discussed in Rule 35. The obligation extends to human rights that apply extraterritorially (Rule 34). If, however, a State interferes with or curtails the exercise or enjoyment of a human right in accordance with Rule 37 on lawful limitations on human rights, or Rule 38 on derogation, it has not violated *lit.* (a).

Nobuyuki Seki of the Tokyo District Court on 9 October 2014 (unreported), (taking into account the *Google* v. *Spain* ruling to support the finding that Google had the obligation to remove search results referring to crimes the complainant might have been involved in over a decade earlier because such search results allegedly threatened his life and privacy.). *See also* Loi No. 78-17 relative à l'informatique, aux fichiers et aux libertés (6 January 1978), Art. 40(I) (Fr.).

[430] Although employing different terminology, this is apparent in ICCPR, Art. 2(1); ICESCR, Art. 2. *See also* General Comment 31, para. 6.

[431] *See, e.g.*, The Right to Privacy in the Digital Age, GA Res. 69/166, para. 4(a), UN Doc. A/RES/69/166 (10 February 2015); UN GGE 2015 Report, para. 28(b); Council of Europe Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users, para. 2 (16 April 2014).

3. A duty to respect human rights is also triggered when a non-State entity's cyber activities are attributable to a State (Rules 15 and 17). For example, a State that instructs, or directs or controls, third parties, like private companies, to collect, retain, or disclose personal data will be responsible for human rights violations that occur in the course of that conduct.

4. *Lit.* (a) must be distinguished from *lit.* (b), which addresses the obligation to protect the international human rights of individuals from abuse by third parties. The International Group of Experts agreed that, pursuant to *lit.* (b), international human rights law entails a general positive obligation requiring States to take action to protect the enjoyment or exercise of rights of those within their territories or territories under their exclusive governmental control, that is, to 'ensure respect' for said rights by others.[432] The Experts concurred that *lit.* (b) obliges States to take action in relation to third parties that is necessary and reasonable in the circumstances to ensure that individuals are able to enjoy their rights online, but that States have discretion with respect to which measures to take in order to satisfy the obligation. For example, assume a third party threatens an individual who expresses certain protected views online. The State where the individual is located has an obligation to protect the individual from the third party's threatened action.

5. The International Group of Experts observed that some States hold the position that the obligation to protect is limited and cannot be characterised as a general obligation of customary international human rights law.[433] Nevertheless, the Experts noted that while, as explained below, the precise parameters of the obligation may be contested, it is reflected in most major international human rights law treaties.[434] The obligation to protect is further recognised in case law, as indicated below

[432] ICCPR, Art. 2(1). *See also* ACHR, Art. 1(1); General Comment No. 3, para. 1; General Comment No. 31, para. 7. *See also, e.g.*, application of the duty to protect in the context of the ECHR in *Case of Osman* v. *United Kingdom* (87/1997/871/1083), judgment, paras. 115–122 (28 October 1998), and of the ACHR in *Velasquez Rodriguez* case, judgment, Inter-AmCtHR (ser. C) No. 4, paras. 166–167 (1988).

[433] *See, e.g.*, Letter from David Bethlehem QC, Legal Adviser, Foreign and Commonwealth Office, to John Ruggie, Special Representative on Human Rights and Transnational Corporations and Other Business Enterprises, Office of the High Commissioner for Human Rights (9 July 2009); Department of State, US Observations on Human Rights Committee General Comment 31, paras. 10–18, 27 December 2007.

[434] *See, e.g.*, ICCPR, Art. 2(1); ACHR, Art. 1(1).

in the commentary. The International Group of Experts was accordingly comfortable in concluding that the obligation is customary in nature.

6. The Experts could not achieve consensus on the precise territorial circumstances in which a State has an obligation to protect a particular individual's human rights from interference by third parties. To illustrate, consider the case of an individual outside a State who hosts his or her website on servers located in the State. Another State hacks into the web server and corrupts the website, thereby interfering with the individual's freedom of expression (Rule 35). A majority of the Experts was of the view that the State shoulders an obligation to protect only when the individuals concerned are within the territory of the State or in territory under its effective control (Rule 34). The remaining Experts took the position that the obligation to protect is also triggered if the international human right concerned is being exercised within territory under the State's effective control, irrespective of whether the individual is located within that territory.

7. Encompassed within the obligation to protect is the duty of States to safeguard individuals from human rights abuses that are initiated in cyberspace, but may affect their rights offline. In complying with this duty, States may, for instance, criminalise conduct and expression, including cyber activities, that harm the rights of others, as in the case of direct and public incitement to genocide;[435] child pornography;[436] and incitement to national, racial, or religious hatred that constitutes incitement to violence.[437] In that regulation in each of these areas restricts the right of freedom of expression (Rule 35), it must comply with the international human rights law obligations relating to limitations discussed in Rule 37.

8. The obligation to protect entails taking measures that are preventive in nature. It is not limited to those necessary to terminate an on-going abuse of human rights by third parties or the taking of appropriate measures against those who have committed such abuse. Accordingly, States are equally obliged to take those feasible measures that are

[435] Genocide Convention, Art. III; Rome Statute, Arts. 3(e), 25; ICTY Statute, Arts. 3(c), 4; ICTR Statute, Arts. 2, 3(c).

[436] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Art. 3, 25 May 2000, 2171 UNTS 227; Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography, para. 2, UN Doc. A/HRC/12/23 (13 July 2009). *See also* Convention on Cybercrime, Art. 9.

[437] ICCPR, Art. 20.

reasonable in the circumstances to prevent an abuse of human rights by third parties if there are reasonable grounds to believe that such abuse will occur.[438] As an example, if a certain ethnic group living in a defined territory in a State has been the target of repeated malicious cyber operations that interfere with the group's members' right to express themselves on political matters on the Internet, the State concerned is obligated to take measures that are feasible and reasonable in the circumstances to preclude future malicious operations of the same nature.

9. The Internet has been used for terrorist purposes, such as recruitment for, incitement of, and the financing of terrorism.[439] The International Group of Experts agreed that 'States have both a right and a duty to take effective measures to counter the destructive impact of terrorism on human rights', even though some measures taken by the State may affect human rights such as the freedom of expression and the right of privacy.[440] Any such measures must comply with Rule 37.[441]

10. The International Group of Experts could achieve no consensus as to whether States have an obligation to ensure access to cyberspace and cyber infrastructure, if such access is the only way to exercise a human right.[442] Consider a situation in which a State has an electoral

[438] *See, e.g.*, *Velasquez Rodriguez* case, judgment, Inter-AmCtHR (ser. C) No. 4, paras. 172, 174–175 (1988).

[439] *See, e.g.*, Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to Resolution 1373 (2001) concerning Counter-terrorism addressed to the President of the Security Council, S/2015/683, at 7–12 (2 September 2015).

[440] United Nations Office on Drugs and Crime, The Use of the Internet for Terrorist Purposes, paras. 33, 80–8 (September 2012); SC Res. 2178, para. 2, UN Doc. S/RES/2178 (24 September 2014) (encouraging 'Member States to employ evidence-based traveller risk assessment and screening procedures including collection and analysis of travel data, without resorting to profiling based on stereotypes founded on grounds of discrimination prohibited by international law'.) *See also Brogan and others* v. *United Kingdom*, judgment, App. No. 11209/84, ECtHR, para. 61.3 (1988); International Code of Conduct for Information Security, Art. 2(4), UN Doc. A/69/723 (13 January 2015); Information Technology Act (9 June 2000), Art. 66F (India); Anti-cyber Crime Law, Royal Decree No. M/17, 8 Rabi 11428 (26 March 2007), Art. 7 (Saudi Arabia).

[441] Inter-American Commission on Human Rights, Report on Terrorism and Human Rights, OEA/Ser.L/V/II.116, Doc. 5 rev. 1 corr., para. 36 (2002); General Comment No. 34, para. 46.

[442] For instance, the obligation to provide access is only framed in hortatory and aspirational terms in the Inter-American Commission on Human Rights, Freedom of Expression and the Internet, para. 37, OEA/ser.L/V/II (31 December 2013).

system requiring individuals to vote online. The Experts were unable to agree if the State is obliged to provide the necessary access to enable individuals who cannot otherwise do so to exercise their right to vote.

11. In order to give effect to the obligation to protect, States have created additional obligations through treaty law. International human rights treaty regimes sometimes obligate States to conduct prompt, effective, thorough, independent, and impartial investigations of alleged human rights violations.[443] A number of treaties require notification and reporting,[444] measures of accountability, and effective remedies for victims of human rights violations.[445] In situations where such obligations exist, any remedies must be known and accessible to those who claim a violation of their rights. All of the Experts recognised that these treaty obligations apply equally to alleged violations of international human rights law perpetrated by cyber means.

12. The Experts did not agree, however, on whether the obligation to provide remedies to victims of international human rights law violations is of a customary nature.[446] The majority was of the view that no such obligation has crystallised, whereas the minority took the opposite position.[447]

13. A few Experts went so far as to assert that the purported customary law obligation to provide an effective remedy for violations of international human rights law that might occur during the collection of electronic communications and personal data through surveillance

[443] *See* Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, GA Res. 60/147, UN Doc. A/RES/60/147 (16 December 2005); General Comment No. 31, paras. 8, 15. *See also* UDHR, Art. 8; ICCPR, Art. 2(3); ACHR, Art. 25; ECHR, Art. 13.

[444] *See, e.g.*, ICCPR, Art. 40 on the periodic reporting requirements of States Parties.

[445] ICCPR, Art. 2(3)(a–b). *See also* General Comment No. 16, para. 11; General Comment No. 31, paras. 8, 15; UN Human Rights Committee, *Dmitriy Vladimirovich Bulgakov* v. *Ukraine*, Communication No. 1803/2008, paras. 9–10, UN Doc. CCPR/C/106/D/1803/2008 (29 November 2012).

[446] *See*, *e.g.*, UN Guiding Principles on Business and Human Rights, Human Rights Council, para. 25, UN Doc. A/HRC/17/31 (16 June 2011). Though the Report is guiding principles, para. 25 provides that 'as part of their *duty* to protect against business-related human rights abuse, States *must* take appropriate steps to ensure . . . those affected have access to effective remedy.' (emphasis added).

[447] UDHR, Art. 8; Basic Principles and Guidelines on the Right to a Remedy and Reparations for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, Arts. 1(b), 2, GA Res. 60/147, UN Doc. A/RES/60/147 (16 December 2005).

programmes necessitates an 'independent oversight body . . . governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society,'[448] to monitor such programmes in the State concerned. The other Experts countered that international human rights law has not developed to the point where any such obligation exists. Rather, the obligation to provide remedies, if any, solely attaches as to individuals to whom human rights obligations are owed and do so only once the violation has taken place. For them, *ex ante* preventive monitoring measures far exceed the requirements of current customary international human rights law.

14. As mentioned above, the text of this Rule incorporates no obligation of States to fulfil human rights, that is, to take measures to ensure that individuals can realise their rights. This is because the International Group of Experts was unable to reach consensus on whether the obligation to fulfil is of a customary nature. However, the Experts noted that some human rights treaties contain an obligation of States Parties to fulfil certain international human rights, in other words, to take measures beyond those required by the obligations to respect and protect. They pointed to the fact that treaty regimes may impose a special obligation to ensure the realisation of human rights by cyber means. For instance, States Parties to the Convention on the Rights of Persons with Disabilities are under a specific obligation to 'promote the availability and use of new technologies, including information and communications technologies . . . suitable for persons with disabilities, giving priority to technologies at an affordable cost,'[449] and to 'promote access for persons with disabilities to new information and communications technologies and systems, including the Internet.'[450]

Rule 37 – Limitations

The obligations to respect and protect international human rights, with the exception of absolute rights, remain subject to certain

[448] 'Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression', issued by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, para. 9 (2013). *See also* The Right to Privacy in the Digital Age, para. 41.

[449] CRPD, Art. 4(1)(g). [450] CRPD, Art. 9 (2)(g).

limitations that are necessary to achieve a legitimate purpose, non-discriminatory, and authorised by law.

1. The International Group of Experts agreed that, as a general matter, the basis for a limitation on the enjoyment or exercise of an international human right must be provided for in international law; the limitation must be necessary to achieve a legitimate purpose; and the limitation must be non-discriminatory. In this regard, international human rights law allows States to limit the enjoyment or exercise of certain human rights in order to protect other rights and to maintain national security and public order,[451] including with respect to activities in cyberspace. For instance, restrictions on the right to seek, receive, and impart information pursuant to Article 19 of the ICCPR must satisfy a tripartite test: they must be provided for by law under the clearest and most precise terms possible, foster a legitimate objective recognised by international law, and be necessary to achieve that objective.[452]

2. This Rule extends to both the obligations to respect and to protect (Rule 36). For instance, if a State gains access to the electronic health records of its citizens, such activity must be based on a recognised limitation to the right of privacy. Similarly, if one State allows another State to remotely examine health records to which it has access, there must be a legitimate basis for doing so, such as a shared national security concern.

3. The International Group of Experts cautioned that the criteria for limitations can vary based on the right or treaty concerned. Therefore, with respect to limitations on treaty rights, first recourse must always be to the treaty itself.

4. International human rights that are absolute in nature are not subject to the limitations set forth in this Rule. The term 'absolute rights', as used in the Rule, refers to those rights that may not be limited by States in any circumstance or for any purpose, such as the freedoms from torture and slavery and the freedom to hold an opinion (Rule 35). The impermissibility of limitations is distinct from the notion of non-derogability (Rule 38). For example, although the freedom to manifest one's religion and the freedom from arbitrary deprivation of life are,

[451] *See, e.g.*, UDHR, Art. 29(2); ICCPR, Arts. 18–19, 21; ASEAN Human Rights Declaration, Art. 8.

[452] ICCPR, Art. 19(3)(b); General Comment No. 34, paras. 21–36.

pursuant to certain treaties,[453] non-derogable in time of public emergency, they are not absolute rights in the sense of this Rule.

5. Limitations are lawful only if they serve a legitimate purpose. Such purposes include the protection of rights and reputations of others, national security, public order, public health, or morals.[454] For instance, countering terrorism is a legitimate purpose that allows States to monitor particular online communications without thereby violating the right to privacy. By contrast, the purpose of putting an end to criticism of the government, whether that criticism manifests online or offline, will seldom, if ever, qualify as a legitimate State purpose justifying interference with the right to freedom of expression.[455]

6. A restriction on cyber activities that might otherwise be protected by international human rights law must be 'necessary', although States enjoy a margin of appreciation in this regard.[456] To illustrate, it is generally considered necessary to restrict the exercise of freedom of expression online or the enjoyment of the right to privacy (Rule 35) in order to eliminate child pornography and child exploitation,[457] protect intellectual property rights,[458] and stop incitement to genocide.[459] The

[453] *See, e.g.,* ICCPR, Arts. 4(2), 6, 18(3).

[454] Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 33, UN Doc. A/HRC/29/32 (22 May 2015). Treaties set forth the allowable limitations for particular rights. As an example, the ACHR acknowledges the appropriateness of restricting freedom of expression as necessary to ensure 'respect for the rights or reputations of others'; 'the protection of national security, public order, or public health or morals'; 'the moral protection of childhood and adolescence'; and to counter 'propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence . . .'. ACHR, Art. 13.

[455] *See* General Comment No. 34, paras. 3, 43.

[456] With regard to the European system, see *Handyside* v. *United Kingdom*, judgment, App. No. 5493/72, ECtHR, para. 48 (1976). *See also Chaparro Alvarez* v. *Ecuador*, 2007 Inter-AmCtHR (ser. C) No. 170, para. 93 (2007).

[457] *See, e.g.*, Convention on Cybercrime, Art. 9; Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, Art. 20(f), 1 July 2010, CETS No. 201; Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and replacing Council Framework Decision 2004/68/JHA, Arts. 18–20 (13 December 2011).

[458] Convention on Cybercrime, Art. 10; WIPO Copyright Treaty, Art. 11, 20 December 1996; Agreement Establishing the Word Trade Organization, Annex 1C: Agreement on Trade-Related Aspects of Intellectual Property Rights, Art. 7, 15 April 1994.

[459] Genocide Convention, Art. III. *See also* Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, paras. 23–25, UN Doc. A/HRC/17/27 (16 May 2011).

International Group of Experts noted that with respect to the mass collection of electronic communications that is not directed at particular individuals, the requirement that the surveillance be a necessary limitation on the right to privacy looms large.[460]

7. While the International Group of Experts agreed that any limitation on international human rights must be necessary for the achievement of a legitimate purpose, the Experts were divided as to whether such measures must also be proportionate as a matter of customary international law. The purported proportionality condition of international human rights law requires that the need for any State interference with human rights in order to meet a legitimate State objective be assessed against the severity of the infringement on human rights.[461] Moreover, proportionality requires that the restriction be the least intrusive means available to achieve that objective.[462] By the notion of proportionality, the mass collection of those individuals' electronic communications to whom the State owes human rights law obligations (Rule 34), as an example, may not be conducted if the State can achieve its legitimate objective by other means that do not implicate international human rights or that are more limited in the extent to which they do so. Nor may the mass collection of data be conducted if its effect on the enjoyment of rights such as privacy is disproportionate relative to the specific purpose for which it is conducted.

8. A few of the Experts held the view that while the principle of proportionality is common to various regional international human rights systems and domestic legal regimes, it has not matured into a requirement of customary international human rights law. They pointed to the objection of some States as to whether limitations on the right to privacy are subject to the requirement of proportionality.[463]

[460] *See, e.g.*, *Uzun* v. *Germany*, judgment, App. No. 35623/05, ECtHR, para. 61 (2010). *See also* The Right to Privacy in the Digital Age, para. 25; Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, para. 59.

[461] *See, e.g.*, General Comment No. 27, paras. 14–16; General Comment 34, para. 34; *Leander* v. *Sweden*, Judgment, App. no. 9248/81, ECtHR, para. 59 (1987).

[462] *Wall* advisory opinion, para. 136; General Comment No. 27, para. 14; General Comment No. 34, para. 34.

[463] *See, e.g.*, Ambassador Keith Harper, Explanation of Position by the Delegation of the United States of America on Resolution Entitled 'The Right to Privacy in the Digital Age', A/HRC/28/L.27, Human Rights Council 28th Sess., 26 March 2015.

Moreover, these Experts noted the practice of various States of imposing limitations on international human rights that, while possibly advancing a legitimate State purpose, appear to be a greater infringement on human rights than justified by that need. An example is the broad banning of NGO activities in response to domestic terrorism that limits, *inter alia*, the freedom of expression. In these Experts' view, a customary international law requirement of proportionality with regard to international human rights limitations may constitute *lex ferenda*, but not, in the current state of affairs, *lex lata*.

9. The majority of the Experts, however, accepted a condition of proportionality. In doing so, they relied heavily on the interpretation given to these norms by the independent bodies created through human rights treaties to monitor their sound application.[464] These Experts emphasised that necessity alone does not suffice to justify limiting obligations under international human rights law. They asserted that it would be incongruent with the object and purpose of limitations on international human rights law to permit a restriction that is necessary, but disproportionate to the State's interest in question. Thus, the least restrictive means must be used to limit a human right, although, again, these Experts agreed that States enjoy a margin of appreciation in this regard.

10. It must be cautioned that measures that are necessary (and proportionate, by the majority criterion) to achieve one legitimate aim may not be so for the purposes of another.[465] To illustrate, temporarily suspending general access to the Internet might be permissible in response to a national security emergency involving widespread cyber operations targeting critical infrastructure (see also Rule 62), but would not be allowable in order to preclude the Internet transmission of, for example, material that infringes on copyright or to impede protests protected by the freedom of expression.[466]

[464] *See, e.g.*, General Comment 34, paras. 34–35. On the requirement of proportionality, *see also Ahmadou Sadio Diallo* judgment, para. 67; *Francesco Madafferi* v. *Australia*, Communication No. 1011/2001, para. 9.2, UN Doc. CCPR/C/81/D/1011/2001 (2004); *M.G.* v. *Germany*, UN Human Rights Committee, Communication No. 1482/2006, para. 10, UN Doc. CCPR/C/93/D/1482/2006 (2008); Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, paras. 15, 17; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 24, UN Doc. A/HRC/17/27 (16 May 2011).

[465] The Right to Privacy in the Digital Age, para. 27.

[466] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 49, UN Doc. A/HRC/17/27 (16 May 2011).

11. Restrictions on cyber activities that are otherwise protected by international human rights law must be non-discriminatory.[467] Discrimination could include distinctions, exclusions, restrictions, or preferences that are based on race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status that has the purpose or effect of nullifying or impairing the recognition, enjoyment, or exercise, on an equal footing, of rights and freedoms.[468] As an illustration, it would be discriminatory to block Internet services to a region populated by a particular ethnic group or to charge users in that area much more for access than users located elsewhere, at least without a legitimate reason such as those discussed earlier.

12. Not every instance of difference in treatment *ipso facto* constitutes discrimination, but differentiation requires an objective and reasonable justification.[469] Consider a case in which unrest and violence has been occurring in an area populated by a particular ethnic group. Social media is being used to orchestrate the violent events. In such a situation, the fact that the measures the State takes to limit access to the social media affect the ethnic group more than other individuals in the State does not constitute unlawful discrimination.

13. The UN Human Rights Committee has noted that '[n]o interference [with a right] can take place except in cases envisaged by the law ... [and] relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted'.[470] In the same vein, the International Group of Experts was of the view that any

[467] UN Charter, Arts. 1, 55; UDHR, Art. 2(1); ICCPR, Arts. 2(1), 26; ICESCR, Art. 2(2); CERD, Art. 2; CEDAW, Art. 2; ACHR, Arts. 1(1), 24; ECHR, Art. 14; ASEAN Human Rights Declaration, Art. 9. *See also* General Comment No. 18, paras. 1–4; Committee on Economic, Social and Cultural Rights, General Comment No. 20: 'Non-Discrimination in Economic, Social and Cultural Rights (Art. 2, para. 2, of the ICESCR)', paras. 2, 7–35, UN Doc. E/C.12/GC/20 (2 July 2009); *Carson and others* v. *United Kingdom*, judgment, App. No. 42184/05, ECtHR, paras. 70–71 (2010); *Juridical Condition and Rights of the Undocumented Migrants*, advisory opinion, OC-18/03, Inter.-AmCtHR (ser. A) No.18, para. 101 (17 September 2003); Inter-American Commission on Human Rights, Freedom of Expression and the Internet, paras. 20–21 (*inter alia*) (13 December 2013); Concluding Observations on the Fourth Periodic Report of the United States of America, Human Rights Committee, UN Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014). *See also* The Right to Privacy in the Digital Age, para. 36.

[468] UDHR, Art. 1(1); ICCPR, Arts. 2(1), 26; ICESCR, Art. 2(2); CERD, Art. 1(1); CEDAW, Art. 1; CPRD, Arts. 1, 5; ACHR, Art. 24; ECHR, Art. 14; General Comment 18, paras. 6–7.

[469] General Comment No. 29, para. 7.

[470] General Comment No. 16, paras. 3, 8.

basis for a restriction must be 'provided', 'established', or 'prescribed by law',[471] and must be precise and clear enough to place affected individuals on notice as to its effect. It must also be accessible to the public.[472] Thus, for instance, legislative restrictions on the exercise of freedom of speech on websites, blogs, and via private electronic communications must be sufficiently descriptive to place those who might be affected by them on notice. Likewise, a law or directive upon which online surveillance is based has to outline the conditions under which the State may engage in the surveillance that implicates the right to privacy.

14. The Experts did not agree, however, as to whether the condition that a limitation be provided or prescribed by law necessarily requires that law to be domestic in character. Some of the Experts were of the view that international law may itself provide or prescribe the grounds for limitation. Other Experts took the position that the limitations must be set forth in domestic law.

Rule 38 – Derogation

A State may derogate from its human rights treaty obligations concerning cyber activities when permitted, and under the conditions established, by the treaty in question.

1. Some human rights treaties permit States to derogate, that is, to temporarily release themselves, in full or in part, from the binding nature of certain obligations contained therein in times of public emergency. The precise conditions under which derogation is permitted are defined by the treaty in question; they are generally narrow. For example, the ICCPR permits derogations from some of its provisions 'in time of public emergency which threatens the life of the nation and the

[471] *See, e.g.*, ICCPR, Arts. 9(1), 12(3), 18(3), 19(3), 22(2); ECHR, Arts. 8–11; ASEAN Human Rights Declaration, Art. 8; UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, paras. 15–18, E/CN.4/1985/4 (28 September 1984). *See also* General Comment No. 16, para. 4; Human Rights Committee, *Antonius Cornelis Van Hulst* v. *Netherlands*, paras. 7.3, 7.7, UN Doc. CCPR/C/82/D/903/1999 (5 November 2004); *Ahmet Yildirim* v. *Turkey*, judgment, App. No. 3111/10, ECtHR, paras. 56–57 (2012).

[472] General Comment No. 34, paras. 24–25. *See also Sunday Times* v. *United Kingdom*, judgment, App. No. 6538/74, ECtHR, para. 49 (1979). The European Court of Human Rights has confirmed this requirement in the context of government surveillance of telephone communications without judicial authorisation. *Zahkarov* v. *Russia*, judgment, App. No. 47143/06, ECtHR, para. 236 *et seq*. (2015).

existence of which is officially proclaimed'.[473] Similarly, the ECHR permits derogation from particular provisions 'in time of war or other public emergency threatening the life of the nation'.[474] The ACHR permits derogation in broader circumstances than permitted by the ICCPR and ECHR, that is, '[i]n time of war, public danger, or other emergency that threatens the independence or security of a State Party' with respect to certain of the rights set forth therein.[475] The International Group of Experts agreed that a treaty's derogation provisions apply to cyber activities for Parties thereto. As an example, if a State derogates from a provision involving freedom of expression in full compliance with the terms of the particular treaty in question, it may, to the extent necessary, block access to or remove online posts that might exacerbate a situation of emergency.

2. Some treaties prohibit derogation that is not strictly required by the exigencies of the situation.[476] For instance, in the situation above, placing some limits on the freedom of expression exercised by cyber means may be acceptable, but, depending on the situation, blocking all such expression may not be permissible. Additionally, the ICCPR prohibits derogations that discriminate solely on the basis of race, colour, sex, language, religion, or social origin.[477] The ICCPR, ACHR, and ECHR also bar derogations that are inconsistent with the States Parties' other international legal obligations.[478]

3. The treaty in question may explicitly exempt certain human rights obligations contained therein from derogation. For instance, the ICCPR prohibits derogation from provisions protecting, *inter alia*, the prohibition of the arbitrary deprivation of life, the prohibition against torture and slavery, the right to recognition as a person before the law, and the right to freedom of thought, conscience and religion.[479] Additionally, the ECHR prohibits derogation from the prohibition of punishment without law even during times of emergency.[480]

[473] ICCPR, Art. 4(1). [474] ECHR, Art. 15(1).
[475] ACHR, Art. 27. However, the list of non-derogable ACHR provisions is broader than those of the ICCPR and ECHR.
[476] *See, e.g.,* ICCPR, Art. 4(1); ECHR, Art. 15(1). [477] ICCPR, Art. 4(1).
[478] ICCPR, Art. 4(1); ECHR, Art. 15(1); ACHR, Art. 27(1). [479] ICCPR, Art. 4(2).
[480] ECHR, Art. 15(2).