Digital Technologies and Human Rights: a Legal Framework

A Briefing Paper
May 2022

International Commission of Jurists

Composed of 60 eminent judges and lawyers from all regions of the world, the International Commission of Jurists (ICJ) promotes and protects human rights through the Rule of Law, by using its unique legal expertise to develop and strengthen national and international justice systems. Established in 1952 and active on the five continents, the ICJ aims to ensure the progressive development and effective implementation of international human rights and international humanitarian law; secure the realization of civil, cultural, economic, political and social rights; safeguard the separation of powers; and guarantee the independence of the judiciary and legal profession.

® Digital Technologies and Human Rights: a Legal Framework

International Commission of Jurists
P.O. Box 91
Rue des Bains 33
Geneva
Switzerland

The ICJ is grateful for the financial support from the Federal Foreign Office, Germany for this project.

Digital Technologies and Human Rights: a Legal Framework

A Briefing Paper
May 2022

Table of Contents

Introduction

The rapid development of new digital and other technologies has spurred a transformation of economic activity across frontiers in the cyberspace. It has contributed to economic improvement of human lives, including in advancing the realization of human rights in many parts of the world. It has expanded the frontiers of human knowledge, science and social interactions in a way that brings deep implications for the political and social fabric of many countries. Human rights advocates have been able to effectively use those technologies to facilitate and expand their communication and action capacity. But while new digital technology may be helpful for the protection of human rights, it also carries real and potential negative impact on the enjoyment of human rights, prompting many in the human rights community to increase their scrutiny over the ways in which they are designed, developed and deployed.

Digital technology, which has as primary applications social media and the internet, in fact comprises a growing set of newly developing technologies that include artificial intelligence (AI), virtual reality, quantum computing and others. Artificial Intelligence is difficult to define with precision, but may be loosely described as a cluster of technologies and techniques, which include some forms of automation, machine learning, algorithmic decision making and neural network processing, based on machine and human input to generate processes and outcomes for decision making.[1] The publication of a number of reports and studies, many in the context of the UN human rights system, has helped in the understanding of the human rights challenges faced by the growing use of digital technologies. However, because of the nature, novelty and ongoing development of technological innovation, the applicable human rights legal framework usually receives in comparison less attention than policy frameworks which do not incorporate a rights-based approach.

This briefing paper is aimed at contributing to the understanding of the international human rights legal framework applicable to the design, development and use of new digital technologies. Consolidating of this material into a single briefing paper will be a useful tool in advocacy efforts aimed at reforming legal and policy frameworks applicable to the design and application of such technologies in a human rights compliant way.

The first part contains an outline of the most salient human rights issues arising from the growing use of digital technologies as identified in public reports, mostly from the UN human rights system. The second part delineates the human rights law standards applicable in addressing the impacts of digital technologies, arising from the use of those technologies by both States and business enterprises. The paper ends with some policy recommendations.

1. Mapping digital technologies and their impact on human rights

The use of digital technologies touches virtually all aspects of life today. Although all internationally recognized human rights can potentially be impacted by the use of digital technologies, much of the public interest and scrutiny has tended to focus on the rights to freedom to expression and information, assembly and association, movement, and right to privacy, and non-discrimination and equal protection.[2] Other human rights often

[1] OECD, *Artificial Intelligence in Society (Summary in English)* (2019); Australia Human Rights Commission, *Human Rights and Technology Final Report* (2021) (Hereinafter *Australia Human Rights Commission Report)*, p. 17.

[2] Australian Human Rights Commission, Ibid., p. 41. See the reports of the International Commission of Jurists including *Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia* (December 2019) (hereinafter ICJ, *Dictating the Internet in Southeast Asia Report*), at: https://www.icj.org/wp-content/uploads/2019/12/Southeast-Asia-Dictating-the-Internet-Publications-Reports-

impacted include rights to fair trial and due process, including fundamental guarantees in criminal proceedings and the rights of the child and migrants.

In identifying impacts, it generally matters more the way a particular technology is shaped or designed than the way and purposes for which it is used so as to affect the legal status of a person and its ability to enjoy rights. However, the two elements are linked. Many times the manner in which a particular AI product is designed and its design itself will have a bear in the way it works. For instance, the design of algorithms for facial recognition technologies with racially biased data input will determine the technology to produce the same outcome when used.

Adverse human rights impacts from the use of digital technologies may arise from the conduct of State agents or private actors or be caused by both, many times jointly or in cooperation. State action alone is the source of negative impacts, some constituting violations of human rights, when adopting laws, policies or taking action purported to protect public order and safety, national security, public health, and the effectiveness of social policies.

Developments in digital technology have served to expand the capacity of many people to more fully exercise their rights to freedom of opinion, expression, assembly, association and political participation. Individuals are now able intensively to access and apply information and communication technologies (ICTs) to organize, coordinate, or hold assemblies online. Social media and live streaming platforms have extended the reach and options for freedom of assembly. Civil society have seen their activities facilitated by online services such as the creation of automated "chatbots" to provide legal aid to protesters facing arrest and the use of social media.[3]

Innovations have also expanded the possibilities of freedom of expression in a variety of forms. Various digital platforms such as Reddit, Wikipedia, YouTube have helped in the formation, expression and sharing of opinions. Facebook, Instagram and TikTok, have played an important role by creating more online space to share, like, comment, and post content on any subject users want.

There have also been some benefits in prevention and holding police and security officials accountable for ill-treatment and other misconduct, as in some countries they must use body cameras, rendering their conduct more transparent. Digital technology has had mixed record when it comes to the administration of justice, as it has in some ways facilitated profiling or short-circuited fair trial rights.[4]

While digital innovations open up or expand opportunities for many, they may also facilitate State repression and human rights violations. Artificial intelligence applications in facial recognition, digital identification and even hacking tools pose complex challenges to the rights to privacy, expression, association, assembly and political participation. These

---

Thematic-reports-2019-ENG.pdf ; *Dictating the Internet: Curtailing Free Expression and Information Online in Cambodia* (November 2021) (hereinafter ICJ, *Dictating the Internet in Cambodia Report*), at: https://www.icj.org/wp-content/uploads/2021/12/ICJ-Dictating-the-Internet_Cambodia_Engl.pdf ; *Dictating the Internet: Curtailing Free Expression and Information Online in Thailand* (April 2021), at: https://www.icj.org/wp-content/uploads/2021/06/Thailand-Dictating-the-Internet-FoE-Publication-2021-ENG.pdf ; *Dictating the Internet: Curtailing Free Expression and Information Online in Vietnam* (December 2020) (hereinafter ICJ, *Dictating the Internet in Vietnam Report*), at: https://www.icj.org/wp-content/uploads/2020/12/Vietnam-Freedom-of-expression-Publications-reports-thematic-reports-2020-ENG.pdf

[3] *Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, UN Human Rights Council, UN Doc. A/HRC/44/24 (24 June 2020), para. 8, at https://undocs.org/A/HRC/44/24.

[4] Ibid., para. 12; *Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age*, Human Rights Council, UN Doc. A/HRC/48/31 (13 September 2021) (hereinafter *Report of the UN High Commissioner on The Right to Privacy in the Digital Age 2021*), paras. 24-25.

negative consequences come from the conduct of State authorities, powerful private actors such as businesses and sometimes from private-public partnerships. This has led the UN Special Rapporteur on rights to freedom of peaceful assembly and association to declare that "for many in civil society, the Internet is no longer a safe place, as they have become the growing targets of surveillance and online violence,"[5] often conducted by State agents, but facilitated by private internet service providers.

1.1. Risks and violations emanating from State conduct

States tend to justify their interference or adoption of restrictions on human rights to assembly and association, expression and information and privacy, by citing reasons of public security and safety. Laws criminalizing access to and use of digital tools usually are framed under the objective of fighting cybercrime, terrorism, misinformation and disinformation, and fake news, including in the context of the COVID 19 pandemic and other threats to public health and safety.[6] Below, an illustrative list of the most common interfering or restrictive conduct carried out or authorized by state agents.

a) Network disruptions and shutdowns.

Internet shutdowns, whether comprehensive, partial, or the throttling (slowing down) of internet access carry particular severe human rights consequences. Such practices are often designed to "intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law."[7] This includes blocking the online information regarding assemblies, shutdown of communication networks, and shutdown of the accounts of the activists and organizers. Many of these disruptions occur in the context of public protests.[8] They jeopardize the ability of individuals to organize themselves and assemble, undermine the communication of those seeking to organize assemblies and reduce possibilities to gather large groups aiming at having a greater reach. Besides suppressing access to information, which is essential for the exercise of the rights to peaceful assembly, association, freedom of expression, and political participation, internet shutdowns and disruptions have broader human rights impacts. Shutdowns also have "severe effects on the ability to realize economic and social rights, given the number of essential activities and services they affect, including access to emergency services, health information, mobile banking, transportation and educational materials."[9]

b) Surveillance using digital tools.

Technological innovations have increased the ability of State authorities to practice surveillance of online activities of individuals and hacking of their devices. They may monitor, for example, the planning and organization of protests and its participants, before

---

[5] *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Ten years protecting civic space worldwide*, Human Rights Council, UN Doc. A/HRC/44/50 (13 May 2020), para. 68, at https://undocs.org/A/HRC/44/50.

[6], *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association* on the *Rights to Freedom of Peaceful Assembly and of Association,* Human Rights Council, UN Doc. A/HRC/41/41 *(*17 May 2019) (hereinafter *Report by the SR on the Rights to Freedom of Peaceful Assembly and of Association*), para. 32-37, at https://undocs.org/A/HRC/41/41. The ICJ has documented and analyzed laws and regulations in Southeast Asian states, Vietnam and in Cambodia. See ICJ, *Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia Report*; ICJ, *Dictating the Internet in Cambodia Report*; and ICJ, *Dictating the Internet in Vietnam Report.* Op. Cit. note 2

[7] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, UN Doc. A/HRC/35/22 (30 March 2017), para. 8, at https://undocs.org/en/A/HRC/35/22.

[8] *Report of the United Nations High Commissioner for Human Rights*, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, Op Cit note 3, para. 19

[9] *Ibid*, para. 20.

they occur, by hacking the digital devices used by those seeking to gather. Digital technologies are also sometimes used to conduct surveillance during protests by using biometrics-based facial recognition and the interception of communications.

Surveillance software is sometimes integrated into links sent to protesters' smartphones, who end up into downloading certain applications designed to infiltrate their contacts, chat messages, phone conversations, photos and videos shared on social media and communication platforms.[10] In addition, some State authorities use hacked devices to create false social media accounts taking the identity of protest organizers while sharing false information.[11] Further, the use of identity catcher to identify mobile phone users (through the International Mobile Subscriber Identity and the International Mobile Station Equipment Identifier devices) allow State's authorities to identify individuals seeking to assemble while gaining direct access to the content of their calls, text messages and websites visited.[12] Online surveillance technologies and interference have a significant impact on human rights and come frequently coupled with or lead to harassment and intimidation, creating fear of reprisals for organizing, participating in protests, or even expressing views.

The use of facial recognition technology may also serve to facilitate racial profiling and enhance discrimination against national, ethnic, religious or racial minorities, LGBTI persons, women or persons with disabilities,[13] when profiling is based on ethnicity, race, national origin, gender, sexual orientation and gender identity or other targeted status grounds. Wrong live identification may also result in interventions within peaceful assemblies by security forces, imposing individuals the suffering of negative as well as unfair consequences.[14]

c) Public surveillance and tracking in context of COVID pandemic.

During the COVID pandemic, expanded surveillance measures have allowed governments to have more access to personal information online, including location and medical data.[15]

In some countries, the mandatory use of contact tracing apps to keep track of individuals' location records during the pandemic, may interfere with individuals' rights to provide consent and withdraw it and constitute a violation of the right to privacy.[16] The increased surveillance and tracing apps is purported to protect public health, but States seldom consider compliance with human rights law standards in the design and implementation of those measures.

d) Online education and child data privacy violation during pandemic. The pandemic has made online education and information sharing necessary, but the use of certain digital technology may violate privacy rights, including of children and strengthen power imbalances between children, parents, technology companies, and governments. Child

[10] See, e.g., Privacy International, *A guide to police surveillance of your devices* (29 June 2021), at: https://privacyinternational.org/long-read/4483/guide-police-surveillance-your-devices.
[11] R*eport of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights Op Cit note 3,* para 24
[12] Ibid., para 28. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2017, Op Cit note 7, para. 22
[13] *Report of the UN High Commissioner on the Impact of New Technologies on Human Rights*, Op Cit note 3, para. 32.
[14] Ibid., para. 47. See also *Report of the UN High Commissioner on The Right to Privacy in the Digital Age*, Op Cit note 4
[15] Report of the Special Rapporteur on the Right to Privacy, United Nations General Assembly, UN Doc. A/76/220 (23 July 2021) (Hereinafter *Report of the Special Rapporteur on Managing Pandemics with Respect to the Right to Privacy*). See generally, International Commission of Jurists, *Human Rights in the Time of COVID-19*: Front and Centre, at https://www.icj.org/human-rights-in-the-time-of-covid-19-front-and-centre/.
[16] *Report of the Special Rapporteur on Managing Pandemics with Respect to the Right to Privacy,* Ibid., paras. 16- 20.

data privacy laws have been waived, under this circumstance, by several governments.[17] Educational institutions have been found to collect and keep data about learning capacity, skills and performance of students or their parents without their consent and use the data in their work. Because education is compulsory, and during the pandemic mobility is restricted, the ability of students or parents to withdraw consent is limited.[18] The main challenge here is to balance the influence of the pandemic, the reliance on online education, and emphasis on child privacy protection.

e) *Digital technology and automation in provision of State services*. As the Special Rapporteur on Contemporary forms of racial discrimination noted the growing use of digital technologies, including AI, may determine outcomes in services relating to employment, education, health care and criminal justice, with the risk of discrimination.[19] The use of automation in the provision of certain public services has caused service disruptions in many countries. Artificial intelligence-based programmes may lead to automated decisions to recover non-existent or inaccurately calculated tax or social benefits debts. It may also lead to the wrong identification of certain persons and groups as potentially more dangerous and the taking of restraining decisions in judicial proceedings or in immigration decisions. For instance, the programmes used by law enforcement officials may have been designed with input that reflects high rates of criminal conduct in certain areas or groups, which may lead to those persons being automatically detected as more "dangerous" and so denied rights or benefits. Similarly, social security and unemployment benefits may be denied on the basis of wrong outcomes achieved by a programme designed with already biased data input. Decisions taken on these bases may violate rights to work, social security or guarantees in criminal proceedings.[20]

1.2. Risks and violations emanating from conduct by businesses and other private actors.

Private actors, especially business enterprises, also have a significant impact on the rights to freedom of opinion, expression, assembly, association, political participation and privacy. They include the dissemination of misinformation, disinformation, hate speech and threats and intimidation, as well as the intensive harvesting of data from users without their consent and as part of their business model.

a) Misinformation, disinformation and "fake-news".

The widescale popularization of social media digital platforms, social messengers, and media online, has made possible the rapid and massive dissemination of opinions and information across frontiers to ever wider audiences. It has allowed too the proliferation of information that is false or inaccurate.[21] The real or perceived neglect of the side of digital platforms to effectively moderate content circulated by users is also one of the causes for the proliferation of misinformation. Misinformation, disinformation and "fake news" cause severe impact on the ability of persons to access genuine information and

[17] Ibid., para. 8
[18] Ibid., paras. 9-10.
[19] Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, United Nations General Assembly, UN Doc, A/HRC/44/57 (18 June 2020) p. 6, at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/151/06/PDF/G2015106.pdf?OpenElement.
[20] *Report of the UN High Commissioner on The Right to Privacy in the Digital Age,* paras 22-33.
[21] False information (or misinformation): False or inaccurate information content, having or was deliberately created and disseminated to mislead people.
Disinformation: Information content or set of information content that is false or inaccurate, created with the deliberate intention to mislead people.
Fake news: Information content fabricated from scratch or extremely inaccurate published on the Internet and formatted to resemble news content legitimate general public"
Definitions proposed by the report *Les lumières à l'Ere Numérique* (2021), Report commissioned by the French Government.

form free opinions, and also undermine the exercise of other human rights, such as the right to health.[22] In certain cases, severe forms of false information carry also hate speech and incitement to violence, entailing risks and violations of human rights.[23] For instance, in Myanmar, starting around 2015, Facebook became to be widely used by military and other leaders to disseminate hate speech and calls to violence against the ethnic minority Rohingya, which is said to be linked to the commission of crimes against humanity against that group.[24]

While it is important that internet companies, like States, apply international human rights standards to their content moderation so as to safeguard the rights to freedom of expression and related fundamental freedoms, certain forms of content moderation may infringe on those rights. But narrowly tailored limitations on the rights in form of carefully designed content moderation with robust safeguards can be an important means to protect other human rights.

Content moderation policies in digital platforms such as Facebook,/Meta twitter and YouTube where they exist, may not be fully consistent with international human rights standards and their effective implementation and monitoring appear to be weak or uneven. The implementation of content policies also raises issues of arbitrariness in content removal or account suspension as content moderation often rely on other users' reports of violations of "community standards.[25] Finally, content moderation, or the lack of it, may also raise legal issues in terms of liability protections enjoyed by internet intermediaries and third parties.[26]

b) Algorithm and artificial intelligence systems bias

One key characteristic of continuously evolving digital media and social platforms is their increasing reliance on algorithms and various applications of artificial intelligence. This reliance allows them to develop distinct functionalities that would otherwise be of limited scope and reach, and their operation requires low expenses for high returns. These algorithm systems operate for instance to gather (harvest) data from users of social media, digital news and sites, communications technology and similar systems to identify preferences, tastes and habits in terms of content and advertisement. Collected data are processed to offer targeted products to specific consumers. Sometimes data is sold or transferred to other entities that use them for other purposes, including political campaigning. Algorithms are designed to identify and disseminate content that may have

[22] International Commission of Jurists, *Living Like People Who Die Slowly: The Need for Right to Health Compliant COVID-19 Responses* (September 2020), pp. 107-113, at https://www.icj.org/icj-new-global-report-shows-that-the-right-to-health-must-be-central-to-state-responses-to-covid-19/. See also Amnesty International, *Silenced and Misinformed, Freedom of Expression in Danger during COVID-19* (2021), at https://www.amnesty.ch/de/themen/coronavirus/dok/2021/zensur-und-falschinformationen-verschaerfen-die-gesundheitskrise/silenced-and-misinformed-freedom-of-expression-in-danger-during-covid-19.pdf.

[23] See *United Nations Strategy and Plan of Action on Hate Speech* (May 2019), at https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf. United Nations Human Rights, *Special Rapporteur on Freedom of Religion or Belief: Hate Speech and Incitement to Hatred or Violence*, at https://www.ohchr.org/en/special-procedures/sr-religion-or-belief/hate-speech-and-incitement-hatred-or-violence.

[24] *Dictating the Internet in Southeast Asia Report*, Op. Cit. note 2, p. 10; BSR, *Human Rights Impact Assessment Facebook in Myanmar***,** October 2018, p. 32, at: https://about.fb.com/news/2018/11/myanmar-hria/. See also *Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar*, United Nations Human Rights Council, September 2018, UN Doc. A/HRC/39/CRP.2, at: https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf.

[25] See Meta, *Our Commitment to Human Rights,* March 2021, at: https://about.fb.com/news/2021/03/our-commitment-to-human-rights/

[26] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, United Nations General Assembly, UN Doc. A/HRC/38/35, 6 April 2018 (Hereinafter *Report of the SR on the Promotion and Protection of the Right to Freedom of Opinion and Expression)*, para. 14, at https://www.undocs.org/A/HRC/38/35.

popular uptake, but many times end up disseminating content that is violent, offensive, or discriminatory.[27]

"Algorithmic systems are also used to influence the findability, visibility and accessibility of the material – meaning what content people see, who they connect with and what groups they find."[28] Such systems may facilitate affiliation and identification of individuals with likeminded groups or persons but can also silence movements, prevent civil society groups from reaching a greater audience and reproduce bias and discrimination. There are important issues related to consent of users to allow their data to be used in this way in algorithm systems, but more generally their right to receive or impart information, including to find and access diversity of independent content, without fear or manipulation may be at stake. These rights are at risk when the content individuals are allowed or prompted to receive is determined by the social media algorithms.

There are also adverse consequences relating to privacy and security. The Special Rapporteur on freedom of assembly and association has highlighted that few digital platforms allow for the use of pseudonyms and impose a real name requirement, without securing encrypted communication.[29]

Artificial intelligence based on algorithm systems that are poorly designed may also cause or contribute to discrimination based on various status. Such is the case of certain systems use in public security surveillance by the police and law enforcement officials that may result in racial profiling.[30]

1.3. Risks and violations emanating from collaboration of public-private actors.

States and companies and their activities are often intertwined in public-private partnerships. Companies may create, transfer and service new technologies to States that then purchase and use them in ways not consistent with international human rights standards.[31] In others cases, private digital companies implement or operate policies or orders from public authorities in contravention of human rights law and standards. This includes instances of computer interference, mobile device hacking, facial recognition, surveillance, content censorship, identification, tracking and partial or full network disruption at the behest of public authorities. While some of these practices were already known by the public, others have emerged or are amplified with the COVID-19 pandemic.

Issues of content moderation in respect of the internet also highlight the potential for digital platforms to knowingly contribute to the dissemination and amplifying of hate speech, defamation and incitement to violence, exacerbating their impact. This has occurred when politicians and military leaders propagate racial and ethnic violence in the

---

[27] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, General Assembly, 2018 A/73/348 paras. 15-32. See also Council of Europe, *Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications*, Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET) (2018); European Parliament, *The impact of algorithms for online content filtering or moderation: "Upload filters"* (2020).

[28] *Report by the SR on the Rights to Freedom of Peaceful Assembly and of Association,* Op Cit note 6, para. 60.

[29] Ibid., para 61. See also *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on the use of encryption and anonymity in digital communication*s, United Nations Human Rights Council, UN Doc. A/HRC/29/32 (22 May 2015), para 47.

[30] See Council of Europe, *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making*, Study by Prof. Frederik Zuiderveen Borgesius (2018), at: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

[31] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on Surveillance and Human Rights*, United Nations General Assembly, UN Doc. A/HRC/41/35 (28 May 2019) (hereinafter *Report of the SR on Surveillance and Human Rights*), para. 48 at https://undocs.org/A/HRC/41/35.

context of social and political confrontations in countries such as Myanmar, which has resulted in the commission of serious violations potentially amounting to crimes under international law.

2. Digital technologies and the international human rights framework

As seen above, digital technologies carry significant human rights risks and impacts, including actual violations or abuses of rights. In addition, these impacts are compounded by the lack of transparency in the process of design, development and deployment of algorithms and of public accountability for designers, developers and operators. There is also typically a lack of consultation or participation by rights holders in technology related processes. [32]

The international human rights law framework applicable to the development and use of these technologies is not always understood by State legislators and policymakers and digital companies, and better knowledge may help to improve the likelihood of rights-compliant laws, policies and specific conduct by States and private actors alike. This section aims at providing an outline of key elements of the international human rights legal framework established in international law as evidenced also in international jurisprudence and practice of human rights authorities.

The human rights framework that applies offline necessarily applies online, in the digital world (or cyberspace). The UN General Assembly and its Human Rights Council have expressly recognized that "the same rights that people have offline must also be protected online".[33] It follows that conduct that violates human rights offline must be recognized as a violation when occurring online. This carries with it the right to effective remedy and reparation both online and offline.[34] In addition, as such conduct is unlawful online, there must be accountability for the States and individuals that perpetrate it.

2.1. A human rights approach to digital technologies

This human rights framework rests on broad principles of accountability, transparency and equality and non-discrimination.[35] Accountability demands from actors in the digital sphere clear lines of responsibility and the provision of information to rights-holders and legitimate public authorities as well as the possibility for these to request information on the development and impacts on digital technologies. It requires also enhanced transparency not only to shareholders and internal stakeholders but to rights-holders and the public at

[32] See e.g., ICJ, *Dictating the Internet in Southeast Asia Report,* Op. Cit. note 2, p. 117.
[33] General Assembly Resolution 75/176 on the Right to privacy in the digital age, UN Doc. A/RES/75/176 (16 December 2020) (hereinafter *Resolution on the Right to Privacy in the Digital Age 2020*); General Assembly Resolution 68/167 on *The right to privacy in the digital age*, UN Doc. A/RES/68/167 (21 January 2014), para. 3, at https://undocs.org/A/RES/68/167; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, UN Doc. A/HRC/32/38 (11 May 2016), para. 6, at https://undocs.org/en/A/HRC/32/38; General Assembly Resolution 26/13 on *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/26/13 (14 July 2014), para. 1, at https://undocs.org/en/A/HRC/RES/26/13; General Assembly Resolution 32/13 on *The promotion, protection and enjoyment of human rights on the Internet*, UN Doc. A/HRC/RES/32/13 (8 April 2016), para. 10, at https://undocs.org/en/A/HRC/RES/32/13.
[34] European Commission, Speech by Commissioner Breton on the Digital Services Act, "*What is prohibited offline must be prohibited online"* (17 January 2022), at https://ec.europa.eu/commission/presscorner/detail/en/speech_22_431.
[35] Report of the Secretary General to the Human Rights Council, *Question of the realization of economic, social and cultural rights in all countries: The role of new technologies for the realization of economic, social and cultural rights*, UN Doc. A/HRC/43/29 (4 March 2020), para. 41, at https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf.

large on the design, development and deployment of algorithms and forms of artificial intelligence, which also must incorporate the principle of non-discrimination. [36]

2.2. Non-discrimination and equality under the law

The enjoyment of human rights without discrimination on any status is a universal and general principle of law and is enshrined in all of the principal international human rights treaties. For instance, article 2 (1) of International Covenant on Civil and Political Rights (ICCPR) sets out an obligation to respect and ensure the Covenant rights "without discrimination of any kind," while article 2(2) of the International Covenant on Economic, Social and Cultural Rights (ICESCR) requires the State "to guarantee that the rights enunciated in the present Covenant will be exercised without discrimination of any kind."

Specific treaties, such as the Convention on the Elimination of all forms of Racial Discrimination, the Convention on the Elimination of all Forms of Discrimination against Women, the Convention on the Rights of Persons with Disabilities contain detailed provisions regarding non-discrimination of their target groups.

But the right to non-discrimination is not just confined to the non-discriminatory protection of human rights. Article 26 of the ICCPR, sets out a general obligation to equality before the law, equal protection of the law, and a non-discriminatory application of (any) law or any state conduct. In other words, it is a free-standing right to non-discrimination in respect of any State action or omission.

Human rights treaties provide for a non-exhaustive list of impermissible grounds of discrimination, which includes the catch-all "other status" to capture groups not explicitly listed. Contemporary developments in international law and standards have provided the identification of additional groups to which non-discrimination applies, so that such grounds clearly include, among others: race, colour, sexual orientation or gender identity, age, gender, religion, language political or other opinion, citizenship, nationality or migration status, national, social or ethnic origin, descent, health status, disability, property, socio-economic status, birth or other status.[37]

Not all distinctions based on status are prohibited, but those which are not based on reasonable and objective criteria and have the effect of impairing the enjoyment of human rights will constitute impermissible and unlawful discrimination.[38] Distinctions based on reasonable and objective criteria are sometimes necessary to realize the objectives of human rights instruments. Therefore, special attention to the position and needs of individuals and groups with specific and special characteristics such as children, women, persons with disabilities, LGBTI persons, ethnic and religious minorities and indigenous people may be allowed. Non-discrimination also requires the consideration of those situations and needs that place people in positions of vulnerability.

The observance of non-discrimination is vital in relation to the design, development and use of digital technology and their embedded artificial intelligence. For instance,

---

[36] *Report of the United Nations High Commissioner for Human Rights on Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, Op Cit note 3, para. 17

[37] UN Committee on Economic, Social and Cultural Rights (CESCR), *General Comment No. 20: Non-discrimination in economic, social and cultural rights* (art. 2, para. 2 of the International Covenant on Economic, Social and Cultural Rights), UN Doc. E/C.12/GC/20 (July 2009), at: https://www.refworld.org/docid/4a60961f2.html.
UN Human Rights Committee, *General Comment no. 37 on the Right of peaceful assembly* (art. 21 of the International Covenant on Civil and Political Rights), UN Doc. CCPR/C/GC/37 (17 September 2020), at: https://digitallibrary.un.org/record/3884725?ln=en.

[38] UN Human Rights Committee, *Zwaan-de Vries v. Netherlands*, Communication No. 182/1984, para. 13.

Committee on the Elimination of Racial Discrimination has recognized the risks of algorithm bias "when AI is used in decision-making in the context of law enforcement."[39] They may reproduce and reinforce biases that lead to discriminatory practices, chiefly because of the prevailing opacity on the design processes, criteria and data input: "discriminatory outcomes of algorithmic profiling can often be less obvious and more difficult to detect than those of human decisions". Technologies such as facial recognition or algorithm systems used for law enforcement, predictive policing (based on historical data from crime in certain locations) or judicial processes, can lead to decisions that are discriminatory and bring with them serious consequences for the enjoyment of other rights.[40]

But racial profiling by law enforcement is not the only discriminatory impact that AI bias can cause. Algorithm bias can also lead to unfavourable decisions and consequences in employment and conditions for employment, access to public services and private services too such as bank loans. Outputs generated by algorithm systems, when the system is fed with historical data reflecting disadvantage or unfavourable treatment on the basis of gender, age, race, ethnicity, nationality, and the other grounds identified above many times also lead to discriminatory decisions that reproduce discrimination on the basis of gender, age, origin or other status.[41]

Beyond design and use of algorithms, equal protection and non-discrimination must be factored in laws and policies concerning access to internet, online entertainment, online public services and similar so that these are delivered on a non-discriminatory basis. When internet or online services relevant for human rights (such as health and education) are delivered with participation of businesses or other private actors, the State should impose minimum or universal service requirements. Online leisure, entertainment and education must be made available and accessible (in language and modality) to persons with disabilities, children, and linguistic minorities and indigenous groups.[42]

When restrictions of rights guaranteed under international human rights treaties are allowed on certain narrowly defined grounds, they should comply with the relevant principles but also be designed and applied without discrimination based on any protected status.[43]

2.3. States' obligation to regulate for the protection of human rights

Although States generally enjoy some discretion as to the means of implementing their international law obligations internally, in many cases human rights treaties require the State to take protective measures in the form of legislation or regulation, in addition to setting up the necessary institutional machinery for safeguarding human rights. State obligations under human rights treaties are generally classified as obligations to respect and guarantee/ ensure (protect and fulfil). Article 2 (2) of ICCPR requires states to "adopt such legislative or other measures as may be necessary to give effect to the rights recognized" in the Covenant. But legislative or regulatory measures are often necessary for states to take positive action to ensure/guarantee human rights. In General Comment

[39] UN Committee on the Elimination of Racial Discrimination, *General Recommendation 36 on Preventing and Combating Racial Profiling by Law Enforcement*, UN Doc. CERD/C/GC/36 (24 November 2020), para 12, at: https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/1_Global/CERD_C_GC_36_9291_E.pdf.
[40] Ibid., paras 33-35.
[41] *Australia Human Rights Commission Report* Op. Cit note 1, p. 107
[42] *Convention on the Rights of Persons with Disabilities*, Treaty Series, vol. 2515, Dec. 2006, see in particular Articles 9 and 30, at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities.
[43] UN Human Rights Committee, *General Comment No. 18: Non-discrimination* (10 November 1989). For instance, it would be a clear violation of the Covenant, if the right to freedom of movement (article 12) were to be restricted "by making distinctions of any kind, such as on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status" UN Human Rights Committee General Comment No. 27: Article 12 on Freedom of Movement (2 November 1999), para 18.

31, the Human Rights Committee clarified that under the ICCPR, States must "adopt legislative, judicial, administrative, educative and other appropriate measures in order to fulfil their legal obligations."[44]

Under the ICESCR, the "Covenant norms must be recognized in appropriate ways within the domestic legal order, appropriate means of redress, or remedies, must be available to any aggrieved individual or group, and appropriate means of ensuring governmental accountability must be put in place."[45]

In the digital age, States not only have a negative obligation to abstain from unduly interfering with the rights of peaceful assembly and of association but also have a positive obligation to facilitate and ensure these rights in accordance with international human rights norms.[46] Those obligations are set out in several international standards , including binding treaties including the Universal Declaration of Human Rights[47] (Art. 20), the International Covenant on Civil and Political Rights[48] (Art. 21-22) and can also be found in the Convention on the Rights of the Child[49] (Art. 15).

and the UN General Assembly have stressed that States have the obligation to respect and fully protect these rights both online and offline,[50] and called upon all States to "ensure that the same rights that individuals have offline, including the rights to freedom of expression, of peaceful assembly and of association, are also fully protected online, in accordance with human rights law."[51]

Legislative or regulatory action is especially important to discharge obligations to protect against conduct from third parties, including business enterprises, that violates or impairs the enjoyment of human rights guaranteed in human rights treaties.

2.4. The obligation to protect extraterritorially

Because the terrain of cyberspace knows no territorial boundaries, it is important to stress that the obligation to protect under international human rights law extends not only territorially, but extraterritorially. Activity in the digital world is by definition borderless, not limited by physical territorial boundaries, potentially reaching and accessible to all anywhere in the world. In addition, human rights are themselves universal and should be enjoyed b all persons, wherever they may be located.

In the digital sphere, persons are particularly vulnerable to human rights violations and abuses, because the capacity of States and private actors alike to interfere with the human rights is heightened in that they are not limited by physical constraints. This carries an

---

[44] UN Human Rights Committee, *General Comment No. 31 on The nature of the general legal obligation imposed on States Parties to the Covenant*, UN. Doc. CCPR/C/21/Rev.1/Add.13 (26 May 2004) (Hereinafter General Comment No. 31), para 7.

[45] UN Committee on Economic, Social, and Cultural Rights, *General Comment No. 9 on Domestic Implementation of the Covenant* (3 December 1998), para.2.

[46] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, United Nations General Assembly, UN Doc. A/HRC/17/27 (16 May 2011), para. 66, at https://undocs.org/en/A/HRC/17/27; Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association on mission to Oman, UN Doc. A/HRC/29/25/Add.1 (27 April 2015), para. 23, at https://undocs.org/A/HRC/29/25/Add.1.

[47] United Nations *Universal Declaration of Human Rights*, Art. 20, 10 December 1948, 217 A (III).

[48] United Nations *International Covenant on Civil and Political Rights*, Art. 21-22, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

[49] United Nations *Convention on the Rights of the Child*, Art. 15, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3.

[50] General Assembly Resolution 38/7 on *The promotion, protection and enjoyment of human rights on the Internet*, UN Doc. A/HRC/RES/38/7 (17 July 2018), para. 1, at https://undocs.org/A/HRC/RES/38/7.

[51] General Assembly Resolution 73/173, *Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association*, A/RES/73/173 (8 January 2019), para. 4, at https://undocs.org/en/A/RES/73/173.

intensification of curtailment or censorship of freedom of expression and information, the spread of disinformation, the surveillance of communications and unauthorized collection of personal data and metadata.

As it stands, States already have obligations under international law to protect human rights extraterritorially, particularly where a State's conduct impacts on the enjoyment of human rights by others outside the State's territory. In addition, States have an obligation to engage in cooperation for the purposes of realizing and promoting rights across borders.

Extraterritorial obligations have been encapsulated in the Maastricht Principles on Extraterritorial Obligations of States in the area of Economic, Social and Cultural Rights[52] and detailed in its legal commentary.[53] These Principles are a synthesis of existing sources and authorities of international human rights law and, while focused explicitly on economic, social and cultural rights, are also broadly applicable to civil and political rights.

In respect of business enterprises and the State's duty to protect, Maastricht principle 24 affirms that "States must take necessary measures to ensure that actors which they are in a position to regulate [...] do not nullify or impair the enjoyment of economic, social and cultural rights. These include administrative, legislative, investigative, adjudicatory and other measures." Principle 25 makes clear that States need to adopt these kinds of measures where:

a) the harm or threat of harm originates or occurs on its territory;
b) where the non-State actor has the nationality of the State concerned;
c) as regards business enterprises, where the corporation, or its parent or controlling company, has its centre of activity, is registered or domiciled, or has its main place of business or substantial business activities, in the State concerned;
d) where there is a reasonable link between the State concerned and the conduct it seeks to regulate, including where relevant aspects of a non-State actor's activities are carried out in that State's territory;
e) where any conduct impairing economic, social and cultural rights constitutes a violation of a peremptory norm of international law. Where such a violation also constitutes a crime under international law, States must exercise universal jurisdiction over those bearing responsibility or lawfully transfer them to an appropriate jurisdiction."

Extraterritorial obligations are expressly or implicitly provided in UN human rights treaties, including in relation to businesses, and are well integrated into the jurisprudence of the UN treaty bodies.[54]

In respect of the ICCPR, the UN Human Rights Committee has affirmed obligations of States under the ICCPR will require them to protect from abuses of rights committed by private persons or entities, including businesses, and that this obligation will extend extraterritorially where the persons are effectively within the power or control of the

[52] Maastricht Principles on Extraterritorial Obligations of States in the area of Economic, Social and Cultural Rights (2013), at: https://www.etoconsortium.org/nc/en/main-navigation/library/maastricht-principles/?tx_drblob_pi1%5BdownloadUid%5D=23
[53] Olivier De Schutter, Asbjørn Eide, Ashfaq Khalfan, Marcos Orellana, Margot Salomon, and Ian Seiderman, 'Commentary to the Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights', *Human Rights Quarterly* 34, 2012, pp. 1084–1169, at: https://www.icj.org/wp-content/uploads/2012/12/HRQMaastricht-Maastricht- Principles-on-ETO.pdf
[54] General Comment No. 31, Op Cit note 44, paras. 8 and 10; UN Committee on Economic, Social and Cultural Rights, *General Comment No.24 on State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities*, UN Doc. E/C.12/GC/24 (2017); UN Committee on the Rights of the Child, *General Comment No. 16 on State Obligations regarding the Impact of the Business Sector on Children's Rights*, UN Doc. CRC/C/GC/16 (2013).

State.[55] Article 2 paragraph 1 of the ICESCR provides an explicit basis for extraterritorial obligations, requiring "each State Party [...]to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures." The CESCR has addressed the extraterritorial application rights in the context of business activities.[56]

The CESCR has stressed that States' obligations "(do) not stop at their territorial borders" and that State parties must "take the steps necessary to prevent human rights violations abroad by corporations domiciled in their territory and/or jurisdiction" whether they are "incorporated under their laws, or had their statutory seat, central administration or principal place of business on the national territory".[57] The Committee highlighted that a State party would be in breach of its obligations "where the violation reveals a failure by the State to take reasonable measures that could have prevented the occurrence of [a corporate abuse]."[58] The CESCR affirmed that States' extraterritorial obligations extend to activities of business entities that occur outside their territories over which they can exercise control, "especially in cases where the remedies available to victims before the domestic courts of the State where the harm occurs are unavailable or ineffective."[59]

Like the CESCR, the Committee on the Rights of the Child has addressed the issue in detail through a General Comment on State obligations regarding the impact of the business sector on rights protected under the Convention on the Rights of the Child.[60] The Committee highlighted that the Convention "does not limit a State's jurisdiction to territory and there is an obligation to "protect the rights of children who may be beyond their territorial borders."[61] It reaffirmed States' obligations to "respect, protect and fulfil children's rights in the context of businesses' extraterritorial activities and operations, provided that there is a reasonable link between the State and the conduct concerned."[62] The Committee said that States must "enable access to effective judicial and non-judicial mechanisms to provide remedy for children and their families whose rights have been violated by business enterprises extraterritorially."

The Committee on the Elimination of Racial Discrimination and the Committee on the Elimination of Discrimination against Women have made similar affirmations regarding the extraterritorial application of their respective Conventions.[63]

2.5 Developments in State regulatory action of the cyberspace

In recent years, some States have been more proactive in taking regulatory and legislative action in respect of the conduct of internet companies. The EU is finalizing two pieces of

[55] Human Rights Committee, General Comment No. 31, Op Cit note 44, paras 8 and 10.
[56] Committee on Economic, Social, and Cultural Rights, *General comment No. 24*
[57] Ibid, at para 26.
[58] Ibid., at para.32.
[59] Ibid., at para 30.
[60] Committee on the Rights of the Child, *General comment No. 16 Op Cit note 54*
[61] Ibid., at para 39.
[62] Ibid., at para 43.
[63] See for example, Committee on the Elimination of Racial Discrimination, *Concluding observations: Canada*, UN Doc. CERD/C/CAN/CO/18 (24 May 2007), para 17, at https://undocs.org/CERD/C/CAN/CO/18; Committee on the Elimination of Discrimination against Women, *Concluding observations on the combined fourth and fifth periodic reports of India*, UN Doc. CEDAW/C/IND/CO/4-5 (24 July 2014), paras. 14-15, at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW/C%20/IND/CO/4-5&Lang=En

legislation, the Digital Services Act (DSA) and the Artificial Intelligence Act, aimed at providing for more accountability and transparency in this area. The ICJ has commented on the drafts notably to highlight their deficits in terms of independent oversight of surveillance and facial recognition, the absence of full prohibition on the use of real time remote biometric identification systems, such as facial recognition with the risk of their use in ways that are not clearly defined by law and may not be strictly necessary and proportionate to a legitimate aim, and (the DSA) would give power to administrative authorities to block and request information from online providers based on an undefined category of "illegal content".[64]

In relation to business enterprises generally, France adopted in 2017 a law on duty of vigilance[65] and was followed in 2021 by Germany.[66] The EU is currently working on its own Directive to impose due diligence obligations to all business enterprises, including technological ones, operating or based in the EU market space.[67]

China, a country which undertakes systematic surveillance of its population, has increased its regulatory activity in recent years. In addition to its Cybersecurity law of 2016, which lacks the most rudimentary human rights safeguards such as the protection of anonymity, a new Personal Information Protection Law, effective from November 2021, requires individuals' information and consent for any personal data collection or storage and provides higher levels of protection of "sensitive data" (including date concerning minors, health and identity). However, those guarantees are subject to sweeping exceptions that are broadly worded, rendering them almost meaningless. New laws drafted during 2021 also purport to protect minors from overexposure to online gaming, videos and similar, but without making distinctions according to needs and stage of development. Further, the role of institutional mechanisms in the oversight and accountability in the implementation of these laws is weak or unclear.[68]

The new wave of regulatory action over provision and access to digital technologies appear to be driven by mostly economic and security concerns ("digital sovereignty" or "national security"), with only minor, if any, consideration of international human rights obligations. There is a risk that economic and security concerns as main drivers will lead to yet greater powers for authorities which may be used to undermine human rights. Another closely linked risk is that through regulation of private digital companies, State authorities may be acting so as to practically avoid public scrutiny. This happens, for instance, when private

---

[64] ICJ, *Comments by the International Commission of Jurists on the proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* (2022), at: https://www.icj.org/eu-artificial-intelligence-and-internet-regulations-must-fully-respect-human-rights-warns-icj/.

[65] LOI n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (Law No. 2017-399 of 27 March 2017 on the corporate duty of vigilance for parent and instructing companies), JO March 28, 2017, text no.1 (inserted in Article L. 225-102-4 of the French Commercial Code), at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034290626/.

[66] Act on Corporate Due Diligence in Supply Chains, Federal Republic of Germany (2021), at: https://www.bmas.de/EN/Services/Press/recent-publications/2021/act-on-corporate-due-diligence-in-supply-chains.html.

[67] *Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive* (EU) 2019/1937, COM/2022/71 final (22 February 2022), at: https://ec.europa.eu/info/publications/proposal-directive-corporate-sustainable-due-diligence-and-annex_en

[68] Access Now Policy Team, "A Closer Look at China's Cybersecurity Law - Cybersecurity, or Something Else?" *Access Now* (13 December 2017), at https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/

Caster, Michael, "Blog: New Data Protection Law Will Not Reign in China's Techno-Authoritarianism," *ARTICLE 19* (25 August 2021), at https://www.article19.org/resources/blog-new-data-protection-law-will-not-reign-in-chinas-techno-authoritarianism/ ; "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021." *DigiChina* (3 Nov. 2021), at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

actors are constrained by authorities to act restricting the exercise of human rights but without the procedural safeguards that would otherwise apply to State agents.

2.6 Restrictions, derogations, and limitations on human rights and freedoms

In this section, this paper covers mainly freedom of expression and information (article 19 ICCPR), freedom of association (article 22 ICCPR), freedom of peaceful assembly (article 21 ICCPR), the right to privacy (article 17 ICCPR) and the right to political participation (article 25 ICCPR), which are rights that are most directly affected online. None of these are absolute rights. Rather, under international human rights law, States may restrict these rights in narrow and exceptional circumstances. There are certain rights- freedom from torture and ill-treatment, most aspects of the right to life, freedom from slavery, the right to legal personhood, among others- which are not subject to derogation or limitation of any kind.

Under the ICCPR, there are two ways in which human rights may be subject to restriction. One is through derogation pursuant to a declared state of emergency under article 4 ICCPR. The other is by means of limitations, the specific terms of which are stated in the ICCPR articles enunciating the particular rights. The detailed explanation and interpretation of the nature and scope of derogations and limitations are set out in the 1984 Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights[69] and in the General Comments of the Human Rights Committee. In particular, the Committee's General Comment 29[70] covers derogations, while the Committee's most recent General Comments addressing limitations are found in General Comment 34 (freedom of expression)[71] and General Comment 37 (freedom of peaceful Assembly).[72]

2.6.1 Derogations

Under article 4 of the ICCPR, any derogation to Covenant rights may only be undertaken pursuant to a declared state of emergency, notified to States Parties through the office of the UN Secretary General, in a situation which threatens the life of the nation. Any such measure must be non-discriminatory, and each derogating measure must be strictly necessary to meet a specific the threat to the life of the nation. Derogations may not violate the principle of non-discrimination and must be temporary measures. Because the States authority to undertake a derogating measure are constrained by the principles of necessity and proportionality, the State will still be generally bound to respect and ensure all rights, even if not in their full scope. As the Human Rights Committee puts it: "[T]he mere fact that a permissible derogation from a specific provision may, of itself, be justified by the exigencies of the situation does not obviate the requirement that specific measures taken pursuant to the derogation must also be shown to be required by the exigencies of the situation. In practice, this will ensure that no provision of the Covenant, however validly derogated from will be entirely inapplicable to the behaviour of a State party."[73]

2.6.2 Limitations

---

[69] *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc. E/CN.4/1985/4 (28 September 1984), at https://www.refworld.org/docid/4672bc122.html.
[70] Human Rights Committee, General Comment No. 29 on States of Emergency (article 4), UN Doc CCPR/C/21/Rev.1/Add.11 (31 August 2001) (Hereinafter *General Comment 29 on States of Emergency*) para 4.
[71] UN Human Rights Committee General Comment No. 34 UN Doc. CCPR/C/GC/34 (12 September 2011).
[72] UN Human Rights Committee, General comment no. 37 on the Right of peaceful assembly Op Cit note 37
[73] *General Comment 29 on States of Emergency* Op Cit note 70, at para 4.

Regarding ordinary limitations to rights not undertaken pursuant to states of emergency, the ICCPR sets out explicit grounds and conditions under which such limitations may be taken, which are generally similar in respect of the rights to freedom of expression, freedom of peaceful assembly and freedom of association. In each instance, limitations will only be permissible if they meet the conditions of legality, are undertaken for one of the specified legitimate purposes; are necessary and proportionate; and are non-discriminatory.

In respect of freedom of expression, ICCPR article 19.3 provides that restrictions of freedom of expression are subject to certain parameters: "shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."

Both article 21 on freedom of peaceful assembly and article 22 on freedom of association provide of possibility of restrictions on similar grounds. For both rights, restrictions must be provided in law and be "necessary in a democratic society in the interest of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights of others". Article 17 (1) on the right to privacy prohibits interferences with privacy that are "arbitrary or unlawful" but contains no express enumeration of the grounds that might be evoked for such interferences. However, the Human Rights Council has affirmed that requirements of necessity and proportionality must be met to meet the requirement of non-arbitrariness.[74]

Irrespective of the differences in constructions across these provisions in ICCPR, the jurisprudence of treaty bodies, regional human rights courts like the European Court of Human Rights applying similar provisions of the European Convention and human rights experts agree on the general applicability of standards of legitimacy, legality, necessity and proportionality to assess the validity of restrictions of rights under the Covenant.[75] Thus, in its General Comment No. 31 on the nature of the general legal obligation on States parties to the Covenant, the Human Rights Committee holds that "Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."[76]

The jurisprudence of the regional courts also affirms the principles of legality, necessity and proportionality in respect of analogous provisions in regional human rights treaties.[77] the application of principles of necessity and proportionality also in other areas such as the right to privacy, as affirmed by the UN Human Rights Council, its Special Rapporteurs and the UN Human Rights Committee."[78]

---

[74] *Resolution on the Right to Privacy in the Digital Age 2020.* Human Rights Council Resolution, UN Doc A/HRC/Res/42/15 on 26 September 2019

[75] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to *Privacy in the Digital Age*, A/HRC/27/37, 2014 paras 22-23

[76] Human Rights Committee, General Comment No. 31, Op Cit note 44, para. 6. See also *Report by the SR on the Rights to Freedom of Peaceful Assembly and of Association,* para. 12.

[77] Inter-American Court of Human Rights. Compulsory registration of journalists (Arts. 13 and 29 American Convention on Human Rights). Advisory Opinion OC-5/85 of 13 November 1985. Series A No. 5, paras 46 and 80

[78] *Report of the SR on Surveillance and Human Rights,* Op Cit note 31, para. 24; *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, General Assembly, UN Doc. A/69/397 (23 September 2014), para. 30, at https://undocs.org/A/69/397; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Op Cit note 29, para. 16-18; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/23/40, para. 24 (17 April 2013), at https://undocs.org/A/HRC/23/40.

The Human Rights Committee has provided greater detail on the permissible limitations in its General Comments on the content of specific rights. In respect of freedom of expression, the Committee has emphasized that the requirement that a restriction be "provided by law" means that it comply with the principle of legality which require laws imposing restrictions on the rights to free expression and opinion must be formulated with enough precision to: (i) enable individuals to ascertain and adjust their conduct; (ii) provide guidance to those charged with implementing the laws to ensure they can clearly identify which types of expression fall under restrictions and not exercise "unfettered discretion" in restricting freedom of expression; and (iii) not contravene other international human rights law or standards.

Additionally, any restriction must, in the express terms of article 19(3), meet the principles of necessity and proportionality, even where the restriction is pursued for a legitimate purpose. The UN Human Rights Committee has clarified that the test of necessity entails limitations must not be imposed where protection can be provided through less restrictive measures, while the test of proportionality ensures that limitations are proportionate to their function, not overbroad and are the "least intrusive instrument amongst others to achieve their protective function".[79] Restrictions must not impair the essence of the rights and be exceptional, in addition to being consistent with other rights recognized under the ICCPR, including non-discrimination and equality.[80]

The right to an effective remedy and reparations must be available and accessible when restrictive measures are designed or applied in a manner inconsistent with the Covenant. In relation to peaceful assembly and association rights that are unduly restricted, the Human Rights Council has called on States to "ensure effective remedies for human rights violations, including those related to the Internet, in accordance with their international obligations."[81]

In application of the aforementioned principles to specific circumstances, some human rights authorities have drawn conclusions as to the permissibility of certain practices in the digital sphere.

a) Shutdowns and other internet restrictions

The Special Rapporteur on the rights to freedom of peaceful assembly and of association has emphasized "that shutdowns and the blocking of entire websites constituted an extreme and disproportionate measure that could not be justified in any circumstance."[82] Similarly, the Special Rapporteur on the right to freedom of opinion and expression, and peers from regional organizations, has stressed that "shutting down entire parts of communications systems […] can never be justified under human rights law."[83]

Shutting down or throttling of internet access would require a clear legal basis[84] and network shutdowns are considered to "invariably fail to meet the standard of necessity,"[85] and so could almost never be lawful. Demonstrations are "events of extraordinary public

[79] Human Rights Committee, *General Comment No. 34*, Op Cit note 71, paras. 25, 26, 33-35. See also General Comment 37 on Freedom of Assembly, Op Cit. note 37, para 36 and ff.; and Human Rights Committee GC 27 Freedom of Movement, Op Cit note 43, paras 12, 13 and 16
[80] General Comment 27Ibid., para 11 and 18
[81] General Assembly, *Resolution 38/7 on The promotion, protection and enjoyment of human rights on the Internet*, UN Doc. A/HRC/RES/38/7 (17 July 2018), para. 6, at https://undocs.org/en/A/HRC/RES/38/7.
[82] *Rights to freedom of peaceful assembly and of association*, Op Cit note 6, para. 52
[83] OSCE, Joint Declaration on Freedom of Expression and Responses to Conflict Situations, para. 4 (c), (4 May 2015), available from https://www.osce.org/fom/154846
[84] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2017, Op Cit note 7, paragraph 9
[85] Ibid., para 14

interest," and thus shall not be intervened with network shutdowns without abundant explanations.[86]

For the Human Rights Committee "any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination system, including systems to support such communication", must comply with article 19, paragraph 3, of ICCPR. However, such restrictions may never be used to justify the "suppression of advocacy for democratic rights."[87]

b) Surveillance and data collection

State authorities frequently invoke reasons of national security or law enforcement, including for counter-terrorism purposes, to justify intrusions in individual and family privacy in the form of surveillance, wire-tapping, interception of communications. These often involve practices of mass and non-specifically targeted data collection operations. National security or law enforcement (as an expression of public order) may be a legitimate objective when established in the law in clear and precise terms, in any event each and every surveillance and data collection measure needs to be shown to be non-discriminatory and necessary and proportionate to a specific national security or public order concerned, as outlined above. The onus is on the Government to demonstrate the interferences are necessary and proportionate to the specific risk being addressed. The OHCHR has concluded that "[m]ass" or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime."[88] Nor will mandatory third party data retention – where governments require information and communication companies to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access –be either necessary nor proportionate. Surveillance for one legitimate purpose for which it is necessary and proportionate may not be so for other purposes.[89] It follows, that these kinds of restrictive measures must be discontinued, unless they can be refined to be more narrowly targeted, so as to be aimed at specific purposes and be necessary and proportionate for those specific purposes.

When considering the consistency with the European Convention of wiretapping of communications in criminal investigations and for reasons of national security, the European Court of Human Rights has set minimum requirements for what should be set out in law, in order to ensure that any interference with private life rights meets standards of legality, necessity and proportionality. These require that the law should set out: "(i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed."[90]

[86] Ibid., para 11
[87] Human Rights Committee General Comment No. 34, Op Cit. note 71, para. 23; and Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, General Assembly, 2018 A/71/373, para. 26
[88] OHCHR Report Privacy in the digital age, 2014, Op Cit. note 75, para 25
[89] Ibid., para 26-27
[90] *Big Brother Watch and Others v UK*, ECtHR, GC, Applications Nos. 58170/13, 62332/14 and 24960/15, 25 May 2021 para. 335. See also, *Roman Zakharov v. Russia*, ECtHR, GC, Application No. 47143/06, 4 December 2015, para. 231.

2.7 Expression that must be suppressed rather than protected

While all kinds of expression are protected under ICCPR article 19, and may be limited only as outlined above, there is one area in which States are not only permitted a limitation but are obligated to impose one. In particular, article 20 of the ICCPR provides for two situations where States are not only permitted to restrict the right to freedom of expression and opinion but are obligated to do so. Article 20 specifically provides that:

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

The UN Human Rights Committee has made clear that articles 19 and 20 of the ICCPR are "compatible with and complement each other" and that the acts prohibited under article 20 are restricted pursuant to article 19(3), and must be justified "in strict conformity" with article 19.[91] In other words, the implementation of legal prohibitions detailed under article 20 must comply with the principles of legality, legitimacy, necessity and proportionality.

Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) similarly prohibits expression which incites "racial hatred or discrimination" – or "hate speech". In the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence ('Rabat Plan of Action') launched in 2013, it was clearly established that in balancing the right to free expression and opinion and the prohibition of hate speech, measures taken by States must also comply strictly with article 19(3).[92]

2.8. Independent oversight, Remedy and Reparation

Accountability in Artificial intelligence-based digital systems requires the author or decision maker to be identified or identifiable, the provisions of reasons or motivations for decisions, and that there is appropriate human oversight and review to correct errors and monitor and oversee the use of AI at the system level.[93] Oversight functions should be entrusted to an independent body, with expert composition, appropriate resources and powers, and to the judiciary when potential infringements of human rights are at stake. Independent oversight is essential, for instance, for addressing the "growing complexity and opacity of the global data environment" and its vast asymmetries. It should include a robust complaint mechanism to empower civil society to enforce the enforcement of privacy safeguards and other rights.[94] In addition, human supervision and decision making should be mandatory when negative impacts on human rights are likely to occur. This measure is predicated on the assumption of a risk-based approach to AI technologies.

Under international law, States have an obligation to provide for access to an effective remedy and reparations under general international law and the major international human rights treaties. Remedies must be effective, accessible, prompt and include full reparation. Full and effective reparation includes compensation, rehabilitation,

---

[91] General Comment 34, Op Cit note 71, paras 50, 52

[92] Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, at: https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf. This has been confirmed by the Special Rapporteur on Freedom of Expression, see *Report of the SR on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, para 7.

[93] Australia Human Rights Commission Report Op Cit note 1, p. 51

[94] *Report of the UN High Commissioner on The Right to Privacy in the Digital Age (2021)*, Op Cit note 4, para 43. According to OHCHR, such oversight bodies include data privacy authorities, consumer protection agencies, sectoral regulators, anti-discrimination bodies and national human rights institutions. Para. 47

restitution, satisfaction and guarantees of non-repetition.[95] The right to an effective remedy and reparation is a general principal of law, and one accepted by all States, including through the consensus adoption of UN Principles and Guidelines on the Right to an Effective Remedy and Reparation.[96]

In respect of the ICCPR rights that are addressed in this paper, the right to a remedy is guaranteed in Article 2 (3) of ICCPR and in all of the other principal human rights treaties. The UN Human Rights Committee has made clear that under article 2(3) remedies must be prompt, accessible, effective and be provided by an independent competent body who decisions need to be enforceable and lead to the outcome of reparations.[97]

When considering the lawfulness of secret surveillance under the European Convention, the European Court of Human Rights has affirmed the importance of judicial review. It has held that, while "the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge, [in] a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, … it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[98] Once surveillance is terminated, notification to the individual is of the essence to ensure effective access to justice against any potential violation.

Similarly, in relation to the position of intermediaries of services that face orders by authorities to block access or take down content, the European Court of Human Rights has held that a system of prior restraint is only acceptable where it is governed by a legal framework that ensures "both tight control over the scope of bans and effective judicial review to prevent any abuse of power." The Court has further stressed that "the judicial review of such a measure, based on a weighing-up of the competing interests at stake …is inconceivable without a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression."[99]

2.9 International human rights framework and private commercial actors

Private commercial actors, in particular business enterprises, have an important and visible role in design, development and deployment of digital technologies. META/Facebook, Amazon, Google, Samsung, Apple, among many others, are leaders in the research and development of cutting-edge digital technologies many times far beyond their usual fields of activity in areas of online commerce, social platforms and computer services. Together with Chinese companies, some of which are State owned enterprises or state sponsored, these companies concentrate among themselves the bulk of the current drive to technological development in the world. Their power and reach have often tempted State authorities to use the enormous bank of data these companies collect and possess, many times to unlawfully interfere with or supress the exercise of human rights.

International human rights standards are also applicable to these actors, should guide their action and serve as the basis for their policies, as recognized by the Human Rights

[95] The Right to a Remedy and Reparation for Gross Human Rights Violation, ICJ Practitioners, Guide No 2, Revised Edition, 2018, available at https://www.icj.org/wp-content/uploads/2018/11/Universal-Right-to-a-Remedy-Publications-Reports-Practitioners-Guides-2018-ENG.pdf . See in particular Principle 3, which under the Principles and Guidelines is applicable to all violations, not only gross and serious violations.
[96] UN Basic Principles and Guidelines and the Right to a Remedy and Reparation for Gross violations of Human Rights Law and Serious Violations of International Humanitarian Law, adopted by UN General Assembly 60/147 of 16 December 2005. Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-and-guidelines-right-remedy-and-reparation
[97] See ICJ Practitioners Guide, Op Cit note 95.
[98] *Big Brother Watch and Others v UK*, Op. Cit. note 90, para. 336
[99] *Ahmet Yildrim v. Turkey*, ECtHR, Application No. 3111/10, 18 December 2012, para. 64.

Council in 2019 and in numerous other occasions.[100] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has also indicated that "human rights law gives companies the tools to articulate and develop policies and processes that respect democratic norms and counter authoritarian demands."[101]

As highlighted above, it is the primary duty of States to protect against human rights impairment and abuses by business enterprises. The UN Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011,[102] have affirmed the obligation of States to protect against such misconduct of business enterprises. They also proclaim that all business enterprises have a responsibility to respect international human rights standards.[103]

Although the responsibility of companies to respect human rights have not been incorporated into an internationally binding instrument, to fulfil their duty to protect human right, States can and should continue imposing human rights or human rights-related legal obligations on companies as over any other actors subject to their jurisdiction. Currently, many States contemplate in their constitutions, statutes or other law, a duty for legal persons (including companies) to respect human rights.

Various Human Rights Council mandate-holders have highlighted the value of the UNGP's guidance for the operations of private digital companies. In its 2018 report, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression summarized several elements of the UNGPs framework, beyond the recognition of businesses' responsibility to respect human rights:

a) "Avoid causing or contributing to adverse human rights impacts and seek to prevent or mitigate such impacts directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts (principle 13);

b) Make high-level policy commitments to respect the human rights of their users (principle 16);

c) Conduct due diligence that identifies, addresses and accounts for actual and potential human rights impacts of their activities, including through regular risk and impact assessments, meaningful consultation with potentially affected groups and other stakeholders, and appropriate follow-up action that mitigates or prevents these impacts (principles 17–19);

d) Engage in prevention and mitigation strategies that respect principles of internationally recognized human rights to the greatest extent possible when faced with conflicting local law requirements (principle 23);

[100] Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Op Cit note 6
[101] *Report of the SR on the Promotion and Protection of the Right to Freedom of Opinion and Expression,* Op Cit note 33
[102] UN General Assembly, Guiding Principles on Business and Human Rights (2011)
[103] United Nations, General Assembly, Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, A/HRC/17/31, annex (21 March 2011), available from https://www.ohchr.org/documents/issues/business/a-hrc-17-31_aev.pdf; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Op Cit note 33, para. 9-10

e) Conduct ongoing review of their efforts to respect rights, including through regular consultation with stakeholders, and frequent, accessible and effective communication with affected groups and the public (principles 20−21);

f) Provide appropriate remediation, including through operational-level grievance mechanisms that users may access without aggravating their "sense of disempowerment" (principles 22, 29 and 31)."

This international framework should be applied to State requests or orders directed to private companies to shutdown communications and networks, which are implemented by private ICTs providers. According to OHCHR, "[t]hese providers could play a role in challenging Internet shutdown requests from governments and keep their customers informed of developments."[104] However, in practice ICT companies rarely oppose orders of internet disruptions by States.

More generally, greater transparency in their operations and links with States is necessary, especially in relation to the design, development and use (including transfer) of artificial intelligence-based products and services, online content regulation, surveillance, among others. In relation to artificial intelligence, OHCHR has recommended *ex ante* and *ex post* impact assessments.[105]

Conclusions

Artificial intelligence- based digital technology has emerged as a critical space for the expanded exercise of human rights thanks to the new accessible and powerful tools embedded in digital platforms. It is also the source of actual and potential violations and abuses of human rights in the hands of State authorities and private companies, particularly where human rights law is not enforced and where adequate protection safeguards are not in place.

International human rights law provides the applicable normative framework to guide the development and application of new technologies and also to provide protective safeguards for these rights, as well as accountability and access to effective remedies and reparations in the case of abuse and violations. But because of the novelty and the rapidly evolving nature of digital technological developments, international human rights law should be complemented with guidance to meet specific challenges such as the human rights risks posed by new uses of artificial intelligence, including automated decision making and machine learning processes, and more specific safeguards and mechanisms of protection.

The UN and regional human rights authorities have considered and clarified in a more refined way the scope of States' human rights obligations in this area. But their approach has been limited by the specificity of their mandates that prevents a holistic approach.

The international human rights framework has also evolved to more clearly encompass now extraterritorial human rights obligations around State regulation, where important challenges still remain in terms of monitoring and enforcement and the discharge of the obligation to provide for access to effective remedies and reparation and accountability. Similarly, in spite of the widespread acceptance of the UNGPS, the enforcement of human

[104] *Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, Op Cit note 3, para. 23

[105] *Report of the UN High Commissioner on The Right to Privacy in the Digital Age* (2021), Op Cit note 4, para 59

rights responsibilities of business enterprises, key actors in the cybersphere, remains very weak.

States and business enterprises have made important progress to understand and comply with their respective human rights obligations and responsibilities as applicable to the cyberspace, but much more is needed. Beyond understanding the applicable human rights framework, States and businesses should double-down their efforts to comply with them and put in place adequate legal and institutional frameworks with the necessary reach across jurisdictions when necessary.

Among the institutions and mechanisms that need to be paid special attention and strengthening are those related to independent oversight of States and private actors' conduct in the process of designing, deploying, and using artificial intelligence in relevant processes and outcomes, as well as independent judicial bodies to deal with violations and abuses of human rights when they occur.

Commission Members

March 2021 (for an updated list, please visit www.icj.org/commission)

President:

Prof. Robert Goldman, United States

Vice-Presidents:

Prof. Carlos Ayala, Venezuela

Justice Radmila Dragicevic-Dicic, Serbia

Executive Committee:

Justice Sir Nicolas Bratza, UK

Dame Silvia Cartwright, New Zealand (Chair)

Justice Martine Comte, France

Ms. Nahla Haidar El Addal, Lebanon

Mr. Shawan Jabarin, Palestine

Ms. Mikiko Otani, Japan

Justice Sanji Monageng, Botswana

Mr Belisário dos Santos Júnior, Brazil

Prof. Marco Sassòli – Italy/Switzerland

Ms. Ambiga Sreenevasan – Malaysia

Other Commission Members:

Professor Kyong-Wahn Ahn, Republic of Korea

Justice Chinara Aidarbekova, Kyrgyzstan

Justice Adolfo Azcuna, Philippines

Ms Hadeel Abdel Aziz, Jordan

Mr Reed Brody, United States

Justice Azhar Cachalia, South Africa

Prof. Miguel Carbonell, Mexico

Justice Moses Chinhengo, Zimbabwe

Prof. Sarah Cleveland, United States

Justice Martine Comte, France

Mr Marzen Darwish, Syria

Mr Gamal Eid, Egypt

Mr Roberto Garretón, Chile

Ms Nahla Haidar El Addal, Lebanon

Prof. Michelo Hansungule, Zambia

Ms Gulnora Ishankanova, Uzbekistan

Ms Imrana Jalal, Fiji

Justice Kalthoum Kennou, Tunisia

Ms Jamesina Essie L. King, Sierra Leone

Prof. César Landa, Peru

Justice Ketil Lund, Norway

Justice Qinisile Mabuza, Swaziland

Justice José Antonio Martín Pallín, Spain

Prof. Juan Méndez, Argentina

Justice Charles Mkandawire, Malawi

Justice Yvonne Mokgoro, South Africa

Justice Tamara Morschakova, Russia

Justice Willly Mutunga, Kenya

Justice Egbert Myjer, Netherlands

Justice John Lawrence O'Meally, Australia

Ms Mikiko Otani, Japan

Justice Fatsah Ouguergouz, Algeria

Dr Jarna Petman, Finland

Prof. Mónica Pinto, Argentina

Prof. Victor Rodriguez Rescia, Costa Rica

Mr Alejandro Salinas Rivera, Chile

Mr Michael Sfard, Israel

Prof. Marco Sassoli, Italy-Switzerland

Justice Ajit Prakash Shah, India Justice

Kalyan Shrestha, Nepal

Ms Ambiga Sreenevasan, Malaysia

Justice Marwan Tashani, Libya

Mr Wilder Tayler, Uruguay

Justice Philippe Texier, France

Justice Lillian Tibatemwa-Ekirikubinza, Uganda

Justice Stefan Trechsel, Switzerland

Prof. Rodrigo Uprimny Yepes, Colombia

International
Commission
of Jurists

P.O. Box 91
Rue des Bains 33
CH 1211 Geneva 8
Switzerland

t +41 22 979 38 00
f +41 22 979 38 01
www.icj.org