ARTICLE 19's submission to the Global Digital Compact's Open Consultation.

ARTICLE 19 welcomes the opportunity to input into the Open Consultation process with a view to the development of the Global Digital Compact, organised by the Office of the United Nations Secretary General's Envoy on Technology.

0. Introduction

As the first and overarching principle, ARTICLE 19 believes that it is essential to take a **human rights-based approach** to the principles and commitments to be set out in the Global Digital Compact (GDC). The GDC needs to reaffirm - as its absolute core principle - that the same rights that apply offline also apply online. The existing international human rights' framework offers a flexible and adaptable baseline for the governance of the digital space. We believe therefore that all existing international human rights commitments[1] must be integrated and mainstreamed as the primary framework throughout all themes and provisions of the GDC. This is particularly vital to realising the vision of the United Nations Secretary-General to "outline shared principles for an open, free and secure digital future for all'[2]. Furthermore, States must ensure complementarity, coherence, and consistency between the GDC and existing international human rights commitments, in order to avoid issuing contradictory and confusing guidance to technology actors.

Second, ARTICLE 19 believes the GDC needs to reaffirm a **multi-stakeholder approach** to governance of the digital space. This requires genuine implementation of the principles of transparency, openness, inclusion, equality, participation, and accountability.

Finally, ARTICLE 19 calls on all relevant actors, including the SG's Envoy on Technology and Member States, to offer unequivocal **clarity** at this point in the process on the drafting modalities, scope and aims/objectives of the GDC, and on the implications and obligations we might expect to see coming out from this process.

[1] International human rights commitments include the Universal Declaration of Human Rights, the core international human rights instruments, and the UN Guiding Principles on Business and Human Rights.
[2] Our Common Agenda - Report of the Secretary-General, p63, https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

1. Connect all people to the Internet, including schools

The impact of Internet connectivity and the extent to which it exists has been widely documented.[3] In recent years, there has been important progress in the international community toward an understanding of connectivity that goes beyond a simple dichotomy of people who technically have access to the Internet and people who do not. In particular, the Office of the United Nations Secretary-General's Envoy on Technology and the International Telecommunication Union (ITU) recently announced new targets that aim to capture a more nuanced standard of connectivity that is "meaningful and universal".[4] This approach clearly recognises that not all government responses to the digital divide are truly inclusive in addressing the diversity of needs and obstacles that different people and communities face.

However, providing universal and meaningful connectivity - which includes "bridging the digital divide" - remains an outstanding problem. Approximately one third of the global population remains unconnected today, and many who have Internet access do not have the quality and types of service to fully exercise their rights online.[5] This is largely because traditional models for expanding connectivity infrastructure rely on the services of incumbent telecommunication network operators, which continue to prioritise access for those who can afford it and deploy infrastructure in areas that will generate the greatest profit.[6] As such, poor, rural, and remote communities that would incur higher deployment costs and provide fewer returns on investment remain unconnected or poorly connected. This problem exists in a broader context in which States deploy strategies and action plans to improve connectivity primarily to fulfil their national social and economic development objectives. Until government approaches to improving connectivity take a rights-based approach, their strategies and models will continue to be insufficient.

Although Internet access in itself is not a human right, it has been recognised as a fundamental enabler of the free and full exercise of all human rights, particularly the right to freedom of expression. Article 19 of the Universal Declaration of Human Rights guarantees the right to freedom of opinion and expression; this right includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media, regardless of frontiers[7]. Access to information is a fundamental component of the right to freedom of expression and must be guaranteed in both online and offline environments[8]. The right to access information is the primary tool that enables the public to access information held by authorities, the media, and other relevant bodies. Internet connectivity enables people to access information held by public authorities, the media, and other relevant bodies. Because access to information also allows for engagement and participatory processes, it directly impacts the exercise of other human rights, such as the right to freedom of association and, after the COVID-19 pandemic, the right to health.[9] In 2016, the UN Human Rights Council affirmed that Member States should formulate national Internet-related public policies that, at their core, ensure universal access and the enjoyment of human rights.[10]

---

[3] https://www.un.org/en/content/digital-cooperation-roadmap/ and https://www.un.org/ohrlls/news/connectivity-least-developed-countries-status-report-2021

[4] https://www.itu.int/hub/2022/04/new-un-targets-chart-path-to-universal-meaningful-connectivity/

[5] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[6] https://a4ai.org/news/new-mobile-broadband-pricing-data-reveals-stalling-progress-on-affordability/

[7] United Nations (1948) Universal Declaration of Human Rights https://www.un.org/en/about-us/universal-declaration-of-human-rights

[8] UN/HRC 2016. The promotion, protection and enjoyment of human rights on the Internet https://digitallibrary.un.org/record/845728?ln=en

[9] Article 19 2020. Viral Lies: Misinformation and the Coronavirus https://www.article19.org/wp-content/uploads/2020/03/Coronavirus-briefing.pdf

[10] https://digitallibrary.un.org/record/845727?ln=en, reaffirmed in 2021, OP15: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G21/173/56/PDF/G2117356.pdf?OpenElement

The lack of connectivity puts populations at greater risk of economic exclusion and being disconnected from essential elements of life, including work, government services, healthcare, and education. A rights-based approach conceptualises connectivity as an enabler of the free and full expression of *all* human rights, including not only economic and social development, but the full breadth of civil and political participation.

Such an approach is necessary to ensure that the UN's targets for meaningful and universal connectivity are truly achieved, as current approaches to addressing connectivity that take a purely economic and social development lens have proven to be limiting. For example, government-backed measures may prioritise infrastructure development in urban and commercial areas or the establishment of community business centres.[11] These approaches ultimately privilege economic producers; by contrast, people and communities who choose not to participate in the mainstream economy or are marginalised or oppressed from doing so due to structural inequalities such as racism or misogyny, are often overlooked. At the same time, connectivity approaches that focus on achieving broad national or regional social and economic development targets may still belie the exclusion of people and communities that rely on connectivity to enable their civil and political participation in ways that may challenge the government or other incumbent powerholders.[12] Under the principles of meaningful and universal connectivity, these people and communities must have robust connectivity as others do.

Moreover, a rights-based approach to connectivity not only addresses the question of which people and communities are connected, but also the nature of the connection itself. Connectivity is only useful if it is designed for the particular needs of people and communities. Needs for robust economic and social participation may not be the same as needs for robust civil and political participation. For example, certain forms of legally protected civil and political participation may require greater reliance on confidentiality, anonymity, and data integrity. The decisions that determine the design, development, and deployment of a network have a fundamental impact on how well these networks enable or undermine efforts by powerholders to carry out surveillance, censorship, or other exploitation or manipulation of the data that people send over these networks once they have connected to the Internet. To ensure that connectivity is truly meaningful and universal, it is necessary to scrutinise the networks that provide this connectivity to determine whether their policies, practices, and technologies enable peoples' rights, particularly to privacy, freedom of expression, and freedom of association.

Recommendations

The GDC must address the protracted problem of the digital divide, and support progress towards achieving meaningful and inclusive connectivity for all. In particular:

- States must affirm in the GDC the relevance of universal and meaningful connectivity as a fundamental enabler of human rights and elaborate on this relevance for the protection, promotion, and enjoyment of civil and political rights, in addition to economic and social

[11] https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.BDR-2020-PDF-E.pdf and https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2020-PDF-E.pdf and https://www.itu.int/en/mediacentre/Pages/pr27-2020-facts-figures-urban-areas-higher-internet-access-than-rural.aspx

[12] Starlink satellites are providing Internet in the Amazon region, which, according to NGOs and experts was key to expand illegal mining activities in the region, increasing the violence against indigenous people and the destruction of the environment in the area. https://www.brasildefato.com.br/2023/02/20/internet-de-elon-musk-e-vendida-a-garimpeiros-da-terra-yanomami-por-compradores-de-ouro-ilegal

Case studies carried out by NGOs in Brazil, Colombia, Kenya and Malaysia showed how the spread of zero rated apps, especially Whatsapp in the Global South, as a strategy to offer cheap connectivity, ended up creating a dependency in the app that was exploited by political campaigners in sharing disinformation https://ourdataourselves.tacticaltech.org/posts/whatsapp/

development. In particular, it must affirm a human rights-based approach to national, regional, and local connectivity expansion and improvement plans.

- States must recognise in the GDC the particular importance of small, community, and non-profit operators in providing complementary connectivity for rural, remote, and other communities that are currently marginalised or overlooked by traditional telecommunication infrastructure development models. Furthermore, it must affirm the creation of an enabling environment that supports small, alternative, and non-profit service providers that operate at the community level, not only large, incumbent telecommunication operators.[13]

2. Avoid Internet fragmentation

It is imperative to ensure that the design, development, and deployment of Internet technologies – from content-layer applications and services to infrastructure-layer protocols and physical devices – enable an open, global, secure, and resilient Internet. In 2022, civil society recorded 187 instances of Internet disruptions in 35 countries.[14] Efforts by both States and companies to block, filter, or throttle access to the Internet – either in whole or in part – contribute to an environment of fragmentation, which fundamentally threatens the free and full expression of human rights, both online and offline.

In 2022, the Office of the High Commissioner for Human Rights (OHCHR) recognised that total Internet shutdowns generally do not meet the principle of proportionality and therefore cannot constitute a legally justifiable restriction on the right to freedom of expression under the international human rights framework.[15] In doing so, the OHCHR echoed the findings of the former UN Special Rapporteur on freedom of opinion and expression in his 2017 report, which unequivocally condemned any measures to intentionally disrupt access to or dissemination of information online.[16] Nevertheless, total internet shutdowns, carried out by States and facilitated by companies, are increasingly being deployed in politically sensitive contexts, including elections and protests, and to conceal and facilitate other grave human rights violations.[17] In some circumstances, such demands are grounded in domestic legislative frameworks, such as those pertaining to emergencies and threats to national security; in others, States apply pressure to, or request the cooperation of, providers to shut down networks in the absence of any applicable regulation.[18]

Clearly, the necessity of the free flow of global Internet communications in the context of international human rights law has been well-established; however, there is an outstanding need for States to actually uphold this norm and hold each other accountable to it.

While total Internet shutdowns are an extreme example of how States and companies contribute to fragmentation, and therefore threaten freedom of expression and other human rights, countries are increasingly relying on blocking entire websites, domains, IP addresses, protocols or services, as well as filtering certain types of content deemed inappropriate or unlawful.[19] These measures may also contribute significantly to Internet fragmentation, cutting off certain people and communities from a truly

[13] https://artigo19.org/2023/02/13/cadernos-de-redes-comunitarias/
[14] https://www.accessnow.org/wp-content/uploads/2023/03/2022-KIO-Report-final.pdf
[15] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/341/55/PDF/G2234155.pdf?OpenElement
[16]
[17] For example, in Iran, India, and Cuba: ARTICLE 19, 'UN: States must stop Internet shutdowns during protests', 1 July 2021, available at: 'https://www.article19.org/resources/un-states-must-stop-internet-shutdowns-during-protests/
[18] See our full policy on shutdowns here: ARTICLE 19, 'Getting connected: Freedom of expression, telcos and ISPs', July 2017, available at: https://www.article19.org/wp-content/uploads/2017/06/Final-Getting-Connected-2.pdf
[19] See the definitions and types of blocking and filtering here: ARTICLE 19, 'Freedom of Expression Unfiltered', 8 December 2018, available at: https://www.article19.org/resources/freedom-of-expression-unfiltered-how-blocking-and-filtering-affect-free-speech/

open and global Internet through technical means that undermine secure and resilient connections. While blocking, filtering, or throttling can be carried out by platforms and websites on which content is shared, service providers across the Internet ecosystem – from applications to infrastructure – have significant powers of blocking, filtering, throttling and moderating content.

Fundamentally, blocking and filtering measures fail to address the offline root causes of the problems that these measures are claimed to address.[20] Blocking and filtering are not only ineffective, but – unless narrowly targeted and compliant with the principles of legality, legitimacy, necessity and proportionality – unlawful under international human rights law.

These measures often lead to over-blocking or 'false positives', and no system can ensure that legitimate content is never wrongfully restricted. In particular, when infrastructure providers are required to implement these types of measures, they are often unable to take targeted actions. If ISPs use address-based blocking, legitimate sites may be blocked because they use the same IP address as "unlawful" sites. If domain name system (DNS) operators or hosting providers flag illegal content, their only recourse is to take down the entire website, including legal content. Conversely, sites containing illegal or targeted content might not be caught by blocking or filtering systems. This is particularly problematic in the case of online child protection, as parents derive a false sense of security from the knowledge that parental control features are in place. These web-based blocks or filters are generally relatively easy to circumvent both by sufficiently tech-savvy end-users and "criminals" when they detect that they have been added to a blocking list.

According to international human rights standards, any blocking or filtering of content must be ordered by a court or other independent adjudicatory bodies. However, in some countries, these orders are given by government departments or other public agencies, sometimes through informal and non-transparent channels. Filtering can occur as a result of legislation that imposes direct obligations on ISPs, DNS operators, social media platforms, and other service providers to block or filter certain types of content. Failure to comply with these obligations is usually punished by sanctions ranging from withdrawal of a license to provide telecommunications services to imprisonment.[21]

Internet providers, either voluntarily or at the behest of governments, can also undermine net neutrality, a key prerequisite to ensuring the equal and non-discriminatory exercise of the rights to freedom of expression and information online. They can restrict, interfere with and discriminate against the network traffic they handle in a variety of different ways. A narrow category of such restrictions is justified under network management, which necessitates prioritising some network traffic for the effective governance of network flows. However, Internet providers often accept payments from platforms and service providers to prioritise content on the basis of origin, destination or service provider, delivering some categories of Internet content at higher speeds, while deliberately slowing or throttling other categories. They can also offer zero-rating arrangements, whereby providers offer access to certain content or services for free and restrict access to other content or services. Governments and legacy telecommunication operators may also impose restrictions on the availability of "over-the-top", IP-based messaging and voice services, which compete with traditional telephony and SMS and may offer encrypted alternatives.

[20] As an example, the incidence of hate speech and online harassment and abuse is rooted in systemic racism, misogyny and wider structural inequities.
[21] For example: ARTICLE 19, 'Tightening the Net', September 2020, available at: https://www.article19.org/ttn-iran-november-shutdown/; ARTICLE 19, 'Navigating Indonesia's Information Highway', March 2013, available at: https://www.article19.org/data/files/Indonesia_Report_ENGLISH.pdf

Recommendations

The GDC must address Internet fragmentation and its threat to human rights. It must especially recognise the role that Internet blocking, filtering, throttling, and total shutdowns play in exacerbating this fragmentation. In particular:

- States must commit in the GDC to ceasing full Internet shutdowns, which are a flagrant violation of the right to freedom of expression, and refraining from imposing filters on content, which should be the decision of the user. Further, they must reaffirm that any blocking measures must be limited in scope, strictly necessary and proportionate to the legitimate aim pursued, provided by law, and only carried out with respect to content that is unlawful or can otherwise be legitimately restricted under international standards on freedom of expression.
- States must commit in the GDC to ceasing actions that place responsibilities on Internet service providers to monitor their networks proactively in order to detect possible illegal content or provide preferential treatment to certain types of content on the basis of origin, destination or service provider.

3. Protect data

Although States have long recognised the importance of data protection in the context of digital technologies,[22] it has been increasingly recognised under the international human rights framework as a necessary principle for the free and full exercise of human rights, both online and offline. In international law, the right to privacy is considered essential in protecting an individual's ability to develop ideas and personal relationships. As such, it enables the enjoyment and exercise of other human rights, including freedom of expression, freedom of association and assembly, and freedom from discrimination. In General Comment 16 of the International Covenant on Civil and Political Rights (ICCPR), the UN Human Rights Committee affirmed that the protection of personal data constitutes a fundamental aspect of the realisation of the right to privacy.[23]

Under international law, data protection encompasses several elements: data collection must abide by principles of fairness and lawfulness; actors responsible for the collection and processing of personal data must ensure it is accurate and, where necessary, kept up-to-date; if personal data is collected, it must serve a specific and legitimate purpose and any such collection must be brought to the knowledge of the data subject; data subjects must have the right to know whether information concerning them is being processed, have the ability to obtain it in an intelligible form without undue delay or expense, and have the ability to take any corrective or remedial action; any collection of data that gives rise to unlawful and arbitrary discrimination must be prohibited; and reasonable and appropriate technical and organisational safeguards must be in place to prevent unauthorised disclosure or breach of data.

As ARTICLE 19 has stated in the context of a range of cases from social media platforms to artificial intelligence, any regulation of technology that does not take into account data protection aspects will prove ineffective in limiting the harmful effects of companies' policies, practices, and business models.[24] It would appear that the international community already understands the importance of strengthening data protection: 80% of States have some form of proposed or enacted data protection legislation.[25] However, among these States, there are an increasing number of cases where such legislative frameworks do not actually protect people and communities, and may even threaten their human

[22] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 45/95, 14 December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm.
[23] https://www.refworld.org/docid/453883f922.html
[24] https://www.article19.org/wp-content/uploads/2021/12/Watching-the-watchmen_FINAL_8-Dec.pdf
[25] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

rights.[26] For example, these frameworks may inappropriately extend the privacy rights of individuals to companies, further entrenching their power and weakening journalists' ability to hold them accountable; fail to include exemptions for artistic, literary, and cultural purposes, as afforded by the right to freedom of expression; and fail to balance data protection with the right to information.[27] Furthermore, States may use the guise of protecting personal data to legitimise 'data localisation' requirements, which disrupt the open, global, secure, and resilient flow of Internet communications by limiting access to social media and other platforms that do not host data within the country's borders and requiring backdoors to surveil data that is hosted locally – in direct violation of the same data protection principles these measures purportedly uphold. Even where data protection frameworks may be compliant with international human rights law and principles, the lack of strong oversight, transparency, or remediation and redress mechanisms may render these laws ineffective in setting meaningful human rights safeguards against government actions.

Recommendations

Any elaboration or reference to data protection in the GDC must centre people and communities and be consistent with international human rights standards and principles, as set out above.

4. Apply human rights online

It is imperative to take a human rights-based approach to the GDC. International human rights commitments must be integrated and mainstreamed as the primary framework throughout all themes and provisions of the GDC. The GDC needs to reaffirm - as its absolute core principle - that the same rights that apply offline also apply online.

The GDC will need to take a "full stack" approach to technology governance, reaching across every level of the modern "technology stack," or the full set of interdependent technologies. This will ensure coherence between regulations addressing the different layers of the technology stack, from manufacturing to infrastructure to content. It is important to note that the relationship between technology, and the right to freedom of expression and other relevant human rights, goes well beyond the world wide web, social media platforms, and applications - the usual well-known targets for regulation. The application of human rights needs to be mainstreamed well beyond the content layer.[28]

ARTICLE 19's Internet infrastructure work demonstrates how the enjoyment of human rights is impacted at lower layers of the Internet, below the "content layer", as well as by digital technologies, especially those which have data-driven elements and are enabled by the Internet. In Brazil for example, ARTICLE 19/ARTIGO 19 championed freedom of expression, right to information, and freedom to association and assembly in the run up to the 2022 general elections. Our organisation campaigned with a view to educating and informing the voting public, outlining how technology can be used to ensure transparency and verify results – as well as highlighting its role in driving disinformation, its vulnerability to hackers, and the increasing use of surveillance tools. This campaign addressed how human rights were impacted by digital technologies that were not strictly the Internet itself but were Internet-connected.[29]

[26] ARTICLE 19's work in East Africa: https://www.article19.org/freedom-of-expression-and-the-digital-environment-in-eastern-africa/
[27] See, e.g. https://www.article19.org/wp-content/uploads/2019/06/Legal-Analysis-of-Draft-Data-Protection-Act.pdf
[28] https://almanac.article19.org/ ; and https://catnip.article19.org/
[29] https://artigo19.org/2022/09/20/confira-nossa-serie-de-videos-especial-sobre-desinformacao-e-eleicoes/

Furthermore, ARTICLE 19 has undertaken in-depth work on biometric technologies (see section 6 on AI). In Mexico, ARTICLE 19/ARTICULO 19, in collaboration with partners, revealed that Pegasus spyware was illegally used to conduct surveillance on journalists and human rights defenders in Mexico from 2019 to 2021, thereby violating their right to privacy, right to freedom of expression and other rights, as well as undermining democratic processes.[30]

Human rights considerations need to be front and centre in decision-making at every stage of technology design, development, manufacturing, standardisation, and deployment. Although governments have the primary responsibility to promote and respect human rights for their citizens, **private sector actors** must enact their responsibilities as well, as per the UN Guiding Principles on Business and Human Rights. In particular, ARTICLE 19 calls on companies to exercise human rights due diligence throughout their operations. In practice, this means that technologies need to be designed in ways that centre the most vulnerable and marginalised communities, rather than treating them like exceptional "edge cases".[31] If this is not the case, real harm risks being perpetrated against these communities. In one glaring example, digital evidence—primarily from device searches—has made it easier for law enforcement to identify, harass, and prosecute LGBTQ people on the basis of their identity. ARTICLE 19 has examined how law enforcement in the MENA region have appropriated and weaponized technology to prosecute queerness, including using photos, dating apps and posts on social media platforms as tools for prosecution.[32] Social media companies in particular need to ensure all their products and services are in line with international human rights law, including data collection practices, and design of recommender systems, and they need to ensure sufficient investment in adequate and context-specific moderation of content in regional contexts.

Governments need to ensure that - national and international - efforts to regulate digital technologies or the "cyberspace" do not violate human rights including freedom of expression. Any limitations need to be strictly compatible with the international human rights framework, including the principles of legitimacy, legality, proportionality and necessity. ARTICLE 19 has documented the use of so-called domestic cybercrime laws to curtail the free enjoyment of human rights, including freedom of expression, media freedom, and right to privacy, including in East Africa[33] and Tunisia[34]. In addition, ARTICLE 19 has consistently raised challenges around platform regulation, where legislative approaches seeking to

[30] https://www.article19.org/resources/mexico-army-spyware-journalists-activists/
[31] "Design from the Margins" is a justice and human rights-centred methodology for how to design technologies. By understanding who is most impacted by social, political and legal frameworks, we can also understand who would be most likely to be a victim of the weaponization of certain technologies. By centering those most impacted, and building from their essential needs, safe and justice-oriented products are created. Using this metric based on the protection of those most marginalised we create better tech for all.
Belfer Center for Science and International Affairs. 2021. Afsaneh Rigot. Available at: https://www.belfercenter.org/person/afsaneh-rigot.
[32] https://cyber.harvard.edu/publication/2022/digital-crime-scenes
[33] https://www.article19.org/wp-content/uploads/2021/02/Freedom-of-Expression-and-the-Digital-Environment-in-Eastern-Africa.pdf
[34] https://www.article19.org/resources/tunisia-cybercrime-law-is-threat-to-free-expression/

"hold social media platforms accountable" are in reality shifting power to platforms to essentially police users' speech, by focusing on regulating content. Any framework that imposes limitations on freedom of expression must be grounded in robust evidence, prioritise the least censorial and restrictive measure, and strictly apply the principles of legality, legitimacy, necessity and proportionality throughout. Rather than tasking platforms to screen and assess all user-generated content, regulators should focus on less intrusive methods that are specifically tailored to tackling some of the negative effects of the platforms' moderation and recommendation systems. For example, regulatory solutions should require companies to be more transparent towards regulators, researchers and users about how their recommendation systems work, set clear limits on the amount of user data that platforms are allowed to collect, and to carry out regular human rights and gender impact assessments to identify and mitigate systemic risks.[35] Furthermore, ARTICLE 19 argues for the need to avoid chokepoints: regulatory interventions must aim to create and safeguard the conditions for open and diverse markets, where power is decentralised rather than concentrated in a few hands and users have viable alternatives to choose from. States should consider pro-competitive remedies as part of their platform regulation frameworks.[36]

At the international level, ARTICLE 19 continues to vigorously push States to limit in scope the proposed cybercrime treaty, currently under negotiation, and to include strong human rights safeguards. The new treaty must not become a tool that states can use against journalists, activists and human rights defenders to stifle free expression.[37] Furthermore, our organisation tirelessly advocates with States to mainstream human rights considerations across all parts of the UN system, in order to ensure coherence and complementarity. This includes anchoring human rights considerations into all relevant resolutions and decisions at the level of the UN General Assembly[38], UN Security Council[39], Human Rights Council[40] as well as intergovernmental processes such as Our Common Agenda (reaching across all its work streams). It requires taking into account and implementing recommendations made by UN Special Procedures and Treaty Bodies. It also requires looking across all thematic areas including when restrictions might be warranted, for example when addressing the misuse of new and emerging technologies by terrorists[41]. These restrictions still need to be consistent with the principles of legitimacy, legality, proportionality and necessity, in order to comply with international law.

[35] https://www.article19.org/wp-content/uploads/2023/01/Watching-the-watchmen-UPDATE-Jan2023-P03c-Interactive-web.pdf
[36] https://www.article19.org/wp-content/uploads/2023/02/Taming-big-tech-UPDATE-Jan2023-P05.pdf
[37] https://www.article19.org/resources/un-cybercrime-treaty-must-not-put-human-rights-at-risk/
[38] E.g. the Right to Privacy in the Digital Age resolution
[39] E.g. relevant resolutions and decisions on counter-terrorism and technology
[40] E.g. New and Emerging Technologies resolution
[41] https://www.justsecurity.org/84246/un-counterterrorism-and-technology-what-role-for-human-rights-in-security/

Recommendation

Governments and private sector actors need to take an unequivocal human rights-based approach across all of the issues addressed in the GDC, as this constitutes the only way we can truly ensure a "free, open, and secure digital future for all".

5. Introduce accountability criteria for discrimination and misleading content

ARTICLE 19 would like to express some concern with the framing and articulation of this topic. For example, it is not clear how we define "accountability criteria for discrimination". In addition, "misleading content" is too vague and will be subject to different interpretations, including articulations that will inevitably lead to crack down of dissent, and violations of media freedom and freedom of expression. We call on all stakeholders to ensure clarity and specificity when setting out topics for the GDC.

If the GDC intends to address the double challenges of discrimination/hate speech and of misinformation/disinformation, it's vital to note that these are not new problems or problems specific to the Internet. Disinformation in particular has in recent years emerged to permeate an increasingly digital society, triggering further debates over politics, journalism and social media. Amid the COVID-19 pandemic, calls to stop the "spread of disinformation" and "infodemics" have increased and more and more States have opted to legislate on the issue. However, sustainable responses to both these challenges must first recognise the need to address the real-world/offline sources of these problems. Full realisation of *all* human rights is the only way to address these challenges effectively. There are a number of international instruments and processes looking at these challenges and we urge the drafters of the GDC to ensure complementarity and coherence.

In general, **governments** need to ensure their regulatory responses to content moderation comply with International Human Rights Law. ARTICLE 19 has outlined clear recommendations on social-media platforms' regulation of content moderation in a way that protects the right to freedom of expression and information. These include rooting any regulatory framework in the overarching principles of transparency, and accountability. It must protect human rights, including respecting rights to non-discrimination and equality, freedom of expression and rights to privacy and data protection, and complying with the principles of legitimacy, legality, proportionality and necessity. Any regulatory framework must be strictly limited in scope. Regulation should focus on illegal rather than 'legal but harmful' content. Private-messaging services and news organisations should be out of scope. Measures should not have extraterritorial application. General monitoring of content must be prohibited. We also believe conditional immunity from liability for third-party content must be maintained, with some clarification on its scope and notice and action procedures. Our full policy can be found on our website.[42]

[42] https://www.article19.org/wp-content/uploads/2021/12/Watching-the-watchmen_FINAL_8-Dec.pdf; and https://www.article19.org/taming-big-tech-protecting-expression-for-all/

In addition, a lot of attention has been dedicated to the relationship between the spread of disinformation and hate speech, and the business models of the largest online platforms, which are profit-driven and where exposure to a wider and diverse range of content is not a priority.[43] This is concerning as plurality and diversity are fundamental in any democratic society as enablers for open and informed public discourse. Despite the larger scale of online information sharing, users are limited in the content they see and access due to the content curation algorithms and practices of the companies. Social media platforms should, in line with their international human rights obligations, ensure full transparency of their decisions and actions concerning how they curate and moderate content, including disinformation and hate speech. Furthermore, ARTICLE 19 recommends States to focus on positive obligations to promote a free, independent, and diverse communications environment, including media diversity and digital and media literacy as key means of addressing disinformation online. States should facilitate access to public information by adopting comprehensive right to information laws and complying with the principles of maximum transparency of public administration.[44]

In the context of the Internet, challenges like hate speech and misinformation/disinformation often impact disproportionately the most marginalised or vulnerable communities; therefore, approaches, practices and rules on content moderation need to adequately consider these communities. ARTICLE 19 conducted research on current practices of content moderation in Bosnia and Herzegovina, Indonesia, and Kenya, with a specific focus on 'harmful content' such as 'hate speech' and disinformation. We have found that social media platforms, rather than serving as spaces for democratic debate and participatory citizenship, have contributed to increasing ethnic-driven disinformation and politically motivated hatred, and reinforcing the exclusion of marginalised groups. Given the importance of social media platforms, in countries where such tensions have in the past caused real-life violence, addressing the weaknesses of content moderation practices is of the utmost importance to ensure sustainable peace and enduring democracies. Under the UN Guiding Principles on Business and Human Rights, companies have obligations to respect human rights and to offer remedy. Social media companies should therefore ensure that decisions on content moderation are made with sufficient awareness and understanding of the linguistic, cultural, social, economic, and political dimensions of the relevant local or regional context.

Finally, existing international human rights law, through article 20(2) of the International Covenant on Civil and Political Rights, effectively regulates the specific case of "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence". We call on the GDC to reinforce and reaffirm these principles, including as laid out 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[45].[46]

[43] https://www.article19.org/taming-big-tech-protecting-expression-for-all/
[44] https://www.article19.org/resources/submission-special-rapporteur-on-freedom-of-expression-and-disinformation/ ARTICLE 19 has also looked at specific contexts of elections in Brazil and Kenya: https://cdt.org/event/a-lie-can-travel-election-disinformation-in-the-united-states-brazil-and-france/; https://www.article19.org/resources/kenya-tackling-misinformation-critical-electoral-integrity/
[45] https://www.article19.org/wp-content/uploads/2018/02/Rabat-Plan-of-Action-OFFICIAL-EN.pdf
[46] In addition, ARTICLE 19 and the Benjamin B. Ferencz Human Rights and Atrocity Prevention (HRAP) Clinic have created an Implementation Assessment Framework for HRC resolution 16/18 with a view to countering religious intolerance, discrimination, and violence on the basis of or in the name of religion or belief more generally.. https://www.article19.org/resources/un-hrc-resolution-16-18-implementation-assessment-framework/

Recommendations

- As restrictions on disinformation de facto limit freedom of expression, any policy or legislative proposal must respect international freedom of expression standards. ARTICLE 19 does not recommend that any legislator use the concept of disinformation to adopt any new legislation, as 'disinformation' and related terms (e.g. 'misinformation,' 'false information' or propaganda) do not have an agreed definition in international human rights law. We also call on the GDC to consider the excellent work delivered by the Special Rapporteur on Freedom of Opinion and Expression on tackling disinformation.[47]
- On hate speech, all responses by governments and private sector actors must comply with existing international human rights standards.

6. Promote regulation of artificial intelligence

Artificial Intelligence (AI) has far-reaching implications for the enjoyment of our human rights in public and private spaces, given its data-intensive nature and application. Moreover, certain AI applications or systems may be fundamentally incompatible with the existing human rights framework.

In 2021, ARTICLE 19 issued a ground-breaking policy on biometric technologies, including facial recognition and emotion recognition technologies, explaining how these impact the enjoyment of our freedom of speech, right to protest, and how they can be used in fundamentally discriminatory ways that disadvantage minorities, vulnerable groups as well as those who have been historically excluded. We called on governments to ban the use of biometric technologies for untargeted mass surveillance in public and publicly accessible spaces and to adopt a human rights-based approach to the design, development, and use of biometric technologies.[48]

Furthermore, we demonstrated how emotion recognition technologies[49] in particular are fundamentally flawed, given their discriminatory and discredited scientific foundations, and have a detrimental impact on human rights, in particular freedom of expression. Concerns are further exacerbated by how they are used to surveil, monitor, control access to opportunities, and impose power, making the use of emotion recognition technologies untenable under international human rights law. ARTICLE 19 therefore recommends States to ban the conception, design, development, deployment, sale, import and export of emotion recognition technologies, in recognition of their fundamental inconsistency with international human rights standards.[50]

[47] https://www.ohchr.org/en/documents/thematic-reports/ahrc4725-disinformation-and-freedom-opinion-and-expression-report; and https://www.ohchr.org/en/documents/thematic-reports/a77288-disinformation-and-freedom-opinion-and-expression-during-armed
[48] https://www.article19.org/wp-content/uploads/2021/05/Biometric-Report-P3-min.pdf
[49] technologies purporting to infer a person's inner emotional state
[50] https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf

Recommendations

Any efforts to regulate the design, development, and deployment of AI technologies, beyond emotion recognition, need to take a rights-based approach and ensure that there are clear safeguards and red lines in place where technologies pose a risk to human rights, meaningful transparency, and meaningful accountability (including appeal and redress mechanisms).[51] States must also build human rights safeguards into the stages of procurement and export of these technologies, through measures ensuring transparency and public consultation, evaluation of human rights impacts, independent oversight and accountability).[52]

[51] https://www.article19.org/wp-content/uploads/2021/12/Civil-Society-Political-statement-on-AI-Act.pdf; https://www.article19.org/resources/europe-artificial-intelligence-act-must-protect-freedom-of-expression-and-privacy/

[52] https://www.article19.org/cctv-myanmar-mass-surveillance/