

\$57, &/ (¶ V V X E P L V V L R Q
W R W K H * O R E D O ' L J L W D O & R P S D F W ¶ V 2 S H Q &

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
R I W K H 8 Q L W H G 1 D W L R Q V 6 H F U H W D U \ * H Q H U D O ¶ V (Q Y R \ R Q 7

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
D S S O \ R Q O L Q H 7 K H H [L V W L Q J L Q W H U Q D W L R Q D O K X P D Q U L J K W V ¶

R S H Q I U H H D Q G V H F X U H ². ~~Further more,~~ I X W X
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.

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

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- E O R F N L Q J R U μ I D O V H S R V L W L Y H V ¶ D Q G Q 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-

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 LQWHUQDWLRQDO ODZ WKH ULJKW WR SULYDF\ LV FRQVLGHUHG H V 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

rights.²⁶ For example, these frameworks may inappropriately extend the privacy rights of individuals to
FRPSDQLHV IXUWKHU HQWUHQFKLQJ WKHLU SRZHU DQG ZHDNHQLQ

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. 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 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 Africa³³ and Tunisia³⁴. 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 <https://www.article19.org/resources/mexico-army-spyware-journalists-activists/>. 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/>

³ KROG VRFLDO PHGR ~~QSWDEWIRUDVHDER~~ UHDOLW\ VKLIWLQJ SRZHU
XVHUV¶ VSHHFK E\ IRFXVLQJ RQ UHJXODWLQJ FRQWHQW \$Q\ IUDI
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.

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, , QGRQHVL D DQG .HQ\D ZLWK D VSHFLILF IRFXV RQ µKDUPIXO 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

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/>