



Joint Declaration on Freedom of Peaceful Assembly and of Association and Misuse of Digital Technologies

Date: 15 September 2023

The United Nations Special Rapporteur on the rights of freedom of peaceful assembly and of association,¹ the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights (IACHR),² the Special Rapporteur on Human Rights Defenders and focal point for reprisals in Africa and Chairperson of the African Commission on Human and Peoples' Rights (ACHPR),³ the Representative of Indonesia to the ASEAN Intergovernmental Commission on Human Rights (AICHR),⁴ and the OSCE Office for Democratic Institutions and Human Rights (ODIHR).

Recalling and reaffirming their Joint Declarations on protecting the right to freedom of peaceful assembly in times of emergencies of September 2022; on protecting and supporting civil society at-risk of December 2021, and on the right to freedom of peaceful assembly and democratic governance of December 2020;

Underscoring the importance of the rights to freedom of peaceful assembly, of association and of expression as essential components of democracy, allowing and empowering everyone in the society, including women, men, young people, children, LGBTI persons, indigenous people, people of African descent, persons with disabilities, and groups vulnerable to discrimination, to participate in decision-making and policy-making processes and shaping their own future;

¹ Mr. Clément Voule.

² Mr. Pedro Vaca.

³ Hon. Rémy Ngoy Lumbu.

⁴ Ms. Yuyun Wahyuningrum.

Stressing again that these rights are fundamental for enabling the full enjoyment and realization of civil, political, economic, social and cultural rights enshrined in the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR); and *acknowledging* that they are vital for upholding democracy, for achieving a just and peaceful society, advancing fair development, and climate justice;

Recognizing that digital technologies are integral to the exercise of the rights to freedom of peaceful assembly, of association and of expression; and *noting* that technologies serves both as a means to facilitate the exercise of the rights to freedom of peaceful assembly, of association and of expression online and offline, and as additional virtual and digitally mediated spaces where these rights can be actively exercised, as stated in the report of the UN Special Rapporteur on the rights to peaceful assembly and association of 2019;⁵

Acknowledging the power of technologies to advance the participation in the democratic space of individuals, civil society, and especially marginalized groups and communities;

Underscoring that the exercise of the rights to freedom of peaceful assembly and of association in the online and offline worlds are complementary and mutually reinforcing, and that the exercise of these rights in either the virtual and digitally mediated spaces or offline sphere does not justify any undue restriction on the exercise of these rights in the other sphere;

Noting that although the digital technologies has opened new space for the enjoyment of the rights to freedom of peaceful assembly, of association and of expression, the digital technologies have also presented additional and evolving threats that severely impede the full realization of these fundamental rights;

Deploring the misuse of digital technologies by State and non-State actors, aimed at suppressing dissent and the curtailing of the effective exercise of these rights online and offline, such as by: imposing Internet shutdowns and censorship, digital surveillance and malicious use of artificial intelligence, online harassment, spread of hate speech, and spread of disinformation and misinformation. Further *condemning* the use of these technologies by State and non-State actors to silence, surveil and harass dissidents, political opposition, human rights defenders, journalists, activists and protesters;

Noting with deep concern that such acts themselves often constitute human rights violations and have serious mental health impact on the victims, as well as to creating a chilling effect and shrinking civic spaces both online and offline, which ultimately threaten the health of a democracy;

Recalling that Internet shutdowns are disproportionate measures and as such constitute a clear violation of the rights to peaceful assembly, of association, and of expression, and can never be considered a legitimate restriction of these fundamental freedoms;

Recognizing that the Internet is a valuable platform enabling Governments to engage with the broader public, especially when seeking solutions to crises; and that it is also important for contributing to ensuring accountability for potential human rights abuses such as when committed in the context of assemblies;

⁵ A/HRC/41/41.

Condemning the spread of disinformation and propaganda over the Internet, which often spread hatred, negative stereotyping or stigmatization, and incitement to violence, discrimination and hostility against those exercising their fundamental freedoms, particularly when States directly sponsor or condone such campaigns;

Noting also that digital technologies and online spaces further exacerbate the impact of hate speech online. *Recognizing* that hate speech seriously impact democracy as it not only affects the directly targeted individuals but the whole group, and undermines the participation and inclusion of all those targeted and affected by it and threatens their fundamental freedoms and rights;

Noting with deep concern that State and Non-State actors are developing and deploying emerging technologies - including artificial intelligence and robotics - in ways that have presented evolving threats and escalated existing risks to human rights, which severely impede the full realization of the fundamental freedoms;

Noting further the lack of basic legal guarantees and effective remedies protecting human rights in the face of the rapid proliferation of surveillance tools. *Stressing* that the use by authorities of digital surveillance, such as spyware, facial recognition and other biometric technologies, and digital profiling tools, poses significant risks to the enjoyment of human rights, including the right to freedom of peaceful assembly and of association, and contributes to the shrinking of civic space and freedom of expression in many countries;

Condemning also the use of commercial spyware, such as FinFisher monitoring technology and the Pegasus spyware, to launch cyberattacks targeting civil society actors, human right defenders, journalists, and all those exercising their fundamental freedoms;

Acknowledging the role and responsibilities of private companies in supplying hacking and surveillance software to governments, that has subsequently been used to target civil society, activists, journalists and human rights defenders; while also *recognizing* the positive role that technical sector (and other private actors) can and should play in addressing these threats.

Expressing further concern about the misuse of artificial intelligence technologies (AI) – such as algorithm-driven systems in content moderation, social media filtering, and surveillance - and the challenges these pose to civic space and democracy; *Noting* that the affordances of algorithmic systems permit the suppression, blocking or promotion of specific content, and the risk that these systems are used to silence or suppress democratic expression and civic engagement in democratic processes.

Noting further that the misuse of these tools often reproduce and reinforce already existing biases and forms of discrimination, and lead to a deepening and proliferation of discriminatory practices against already marginalized or at-risk groups, including women, members of religious minorities, ethnic minorities, and gender and sexual minorities;

Condemning strongly online attacks, including sexual and gender-based violence and abuse of individuals engaging in public debate; and *underlining* the need for gender-sensitive responses that take into account the particular forms of discrimination online and digital privacy;

Noting further the persistence of the digital divides and unequal access to technologies, and limited digital literacy that exacerbate existing inequalities, making it challenging for marginalized communities, including women, youth, persons with disabilities, and minority groups, to exercise their rights to freedom of peaceful assembly, of association and of expression both online and offline;

Expressing concern over the deliberate misuse in application and use of vague and broad laws such as cybersecurity-related laws, antiterrorism laws, surveillance laws, hate speech laws, and disinformation laws, to target and criminalize civil society activists, journalists and protesters, resulting in deepening authoritarian practices, and restricting civic space and fundamental freedoms;

Expressing further concern over the lack of regulation and transparency on the use of digital technologies in policing in many States, in particular in relation to the exercise of the rights to peaceful assembly and of association;

Stressing the need for transparency, accountability, and oversight to make the online spaces open, safe and secure for everyone, without unduly burdening the exercise of these rights;

Reiterating that States must fully comply with their human rights obligations both online and offline, including with reference to the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR); and also with reference to the United Nations Human Rights Council resolutions 38/7 of 2018 and 47/16 of 2021 on the promotion, protection and enjoyment of human rights on the Internet; 48/4 of 2021 and 42/15 of 2019 on the right to privacy in the digital age; 76/227 of 2022 on countering disinformation for the promotion and protection of human rights and fundamental freedoms; the United Nations General Assembly resolutions 77/150 of 2022 on Information and communications technologies for sustainable development; as well as with reference to regional treaties, including the American Convention on Human Rights, the African Charter on Human and Peoples' Rights and its Maputo Protocol, and the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the ASEAN Human Rights Declaration; and regional resolutions, of the African Commission on Human and Peoples' Rights, Resolution ACHPR/Res. 362(LIX) 2016 on the Right to Freedom of Information and Expression on the Internet in Africa, the OAS General Assembly Resolutions AG/RES. 2976 (LI-O/21) on promotion of the rights to freedom of expression, of peaceful assembly, and of association in the Americas and AG/RES. 2928 (XL VIII-O/18) on freedom of expression and internet on electoral contexts; the OSCE Human Dimension Commitments on Freedom of Peaceful Assembly and of Association: Copenhagen Document 1990, Paris Charter 1990, Helsinki 2008, and the Council of Europe Recommendations of the Committee of Ministers to Member States: CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression; CM/Rec(2022)6 on protecting youth civil society and young people, and supporting their participation in democratic processes; CM/Rec(2020)1 on the human rights impacts of algorithmic systems; CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries;

Welcoming and encouraging further efforts by the international community and regional bodies aimed at developing guidance and legal frameworks to address the protection of these rights in the use of digital technologies;

Reiterating also that private companies should comply with international human rights law and the UN Guiding Principle on Business and Human Rights, as well as regional standards such as the Council of Europe Recommendation CM/Rec(2016)3 on Human Rights and Business, and ensure responsibility, accountability and due diligence for how commercial products are used, including by ensuring their

platforms and tools are not used to target, surveil, intimidate, spread hate speech and incite violence including against civil society, activists, and organizers or participants in assemblies;

Adopt, on 15 September 2023, the following Joint Declaration on the rights to freedom of peaceful assembly and of association and the misuse of digital technologies, aiming at ensuring that these rights are facilitated, protected and promoted, and are not suppressed through the use of digital technologies:

General Principles

1. The exercise of the rights to peaceful assembly, of association and of expression are protected under international human rights law online as well as offline or a combination thereof.
2. The rights to freedom of peaceful assembly, of association and expression online should be enjoyed by everyone, without discrimination on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
3. The right to privacy remains an important “gateway” right that reinforces other rights, online and offline, including the rights to freedom of peaceful assembly and of association, and States should protect the right to privacy in digital technologies.
4. Technologies should be used as a means to facilitate the exercise of the rights to freedom of peaceful assembly, of association and of expression offline and online and not to suppress or unduly restrict these rights.
5. States have positive obligations to ensure and facilitate an open, safe, secure, accessible and inclusive digital environment that facilitates the rights to freedom of peaceful assembly and association of individuals and groups.
6. The freedom to access and use digital technologies for the exercise of the rights to freedom of peaceful assembly, of association and of expression rights should be viewed as the rule, and any limitations as the ultimate exception. Restrictions on exercising the rights to freedom of peaceful assembly, of association and of expression online and offline, or a combination thereof, should meet the strict requirements of legality, legitimacy, and necessity and proportionality, and non-discrimination.
7. Measures adopted online or offline for the protection of national security, public order and public health, or in the context of public emergencies, should be in full compliance with international human rights law obligations and should not unlawfully infringe upon the rights to freedom of peaceful assembly, of association and of expression.
8. States must protect against human rights abuse committed by companies operating within their territory and/or jurisdiction; and take appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication; and ensure that victims have access to effective remedies.
9. Companies should meet their responsibility to respect human rights, including the rights to freedom of peaceful assembly and of association offline and online, to ensure that they do not cause, contribute to, or become complicit in undue restrictions or human rights abuses related to the

exercise of these freedoms, and to ensure that the legitimate activities of human rights defenders are not obstructed.

10. Transparent, inclusive and meaningful public consultations should be built-in all governance mechanisms for digital technologies at all stages - from the design to development, deployment, evaluation, rulemaking on the use of technologies, and retirement, taking into consideration the impact they have on the exercise of these fundamental freedoms.

Internet Censorship and Shutdowns

States should:

11. Refrain from and cease shutdowns or disruptions of Internet or telecommunications networks in all circumstances. Internet shutdown is inherently disproportionate, given the blanket nature of the act, which violates the requirement of necessity and proportionality set out in international human rights law.
12. Repeal or amend national laws and policies that permit illegitimate disruptions and shutdowns, ensuring compliance with international human rights law and standards; and refrain from adopting any such laws and policies in the future.
13. Protect and actively facilitate access to the Internet, in line with the right to access to information, recognizing its importance to facilitate the right to participation in political and public life, ensure transparency and accountability, and access to diverse information.
14. Ensure that legislation defining restrictions of online content is exceptional and its application, including in relation to content moderation and curation policies, is consistent with human rights standards, including the rights to freedom of peaceful assembly, of association and freedom of expression, as well as due process rights.
15. Ensure that any decision to block access to digital platforms or content is transparent, subject to judicial review; and justify how such decisions are compatible with States' obligations to respect, fulfil and protect the rights to freedom of peaceful assembly, of association and of expression under international and regional human rights instruments. Any restrictive measures must be subjected to a strict balance of proportionality and be carefully designed and clearly limited so not to affect legitimate speech that deserved protection.
16. As the Internet continues to provide essential tools for taking part in activities and discussions including governance, matters of public interest, crisis management, and conflict prevention and peace-making, ensure virtual spaces are open, safe and accessible, and facilitate free flow of information, at all times, including during public emergencies and conflict.
17. Revise and amend cybercrime, surveillance and antiterrorism laws, bringing them into compliance with international human rights norms and standards governing the rights to privacy, to freedom of peaceful assembly, of association and of expression.

Companies should:

18. Internet service providers and intermediaries must not unduly restrict the rights to freedom of peaceful assembly, of association and of expression, or the right to privacy, including of assembly participants. Any restrictions on the operation of information dissemination systems must conform with the tests for legitimate restrictions on freedom of expression under international human rights law.

Digital Surveillance Technologies

States should:

19. Refrain from and cease the practice of unnecessary and disproportionate surveillance of those exercising their rights to peaceful assembly, of association and expression, in both physical and online spaces.
20. Put in place strict privacy and data protection laws that regulate the collection, retention, analysis and otherwise processing of personal data or information that can categorise individuals or otherwise implicate their rights either at the point of collection or in the future. Ensure that private companies delete illegitimately acquired biometric data.
21. Ensure that surveillance measures and the use of surveillance tools are strictly based on international human rights law and norms. Any surveillance against individuals exercising their rights of peaceful assembly and association may only be conducted on a targeted basis, providing objective standards of that there is a reasonable suspicion that actors are engaging in or planning to engage in serious criminal offences, and under the strict compliance with the principles of legality, necessity and proportionality and providing for close judicial or equivalent standards of supervision.
22. Refrain from recording and retaining footage of assembly participants, unless there are legitimate and specific indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards that conform to international human rights standards.
23. Ensure that law enforcement are provided with robust and clear protocols incorporating international human rights standards, and are effectively trained, on the facilitation, respect and protection of the rights to freedom of peaceful assembly and of association online and offline while using surveillance technologies. Such protocols should outline command responsibility in the decision-making on the use of such surveillance technologies. Ensure appropriate accountability measures are put in place with regards to misuse of surveillance technologies by law enforcement including with regards to the exercise of the rights to freedom of peaceful assembly, of association and of expression.
24. Respect the right to privacy online and offline and facilitate secure, safe and confidential communications, the protection of anonymous speech, and ensure that any interference with the right to privacy, including by communications surveillance and intelligence-sharing, complies with international human rights law, including the requirement of legality, legitimacy, necessity and proportionality.
25. Ensure that companies operating within their jurisdiction or from abroad do not impact negatively on the work of human rights defenders, activists, protesters and journalists through their surveillance products and services, in compliance with the UN Guiding Principle on Business and Human Rights.
26. Impose a global moratorium on the sale, transfer and use of spyware tools until adequate safeguards to protect human rights and fundamental freedoms are in place.
27. Support the development and implementation of a global framework regulating the use of digital surveillance, in accordance with international human rights standards.
28. Put in place robust and accountable export control regimes for surveillance technologies that pose serious risks to human rights, including the rights to freedom of peaceful assembly, of association and of expression.

Mis/Disinformation

States should:

29. Ensure that national authorities refrain from generating, sponsoring, condoning, or disseminating statements which they know or reasonably should know to be false.
30. End all acts of government-sponsored online trolling, intimidation and disinformation targeted at civil society, human rights defenders, protest actors and journalists.
31. Take measures to counter the dissemination of disinformation, as appropriate, and in accordance with international human rights law. Refrain from enacting vague and overbroad laws such as to combat 'fake news' and ensure that any such existing laws and policies are not used to target civil society actors, journalists, citizens journalists and others, and do not unreasonably restrict the individuals' freedoms of expression and freedom to seek, receive and impart information.
32. Require greater transparency, accountability and global responsibility from online platforms around mis/disinformation affecting peaceful assembly and association rights.
33. Prioritize the protection of discriminated and marginalized groups and activists defending their rights, who are disproportionately subjected to the harmful effects of mis/disinformation.
34. Support the development of a multi-pronged approach requiring global and regional cooperation by a range of stakeholders to safeguard persons involved in peaceful protests, independent media and civil society organizations, from the harms that stem from mis/disinformation.
35. Support and facilitate independent research, in collaboration with civil society and academics, on the drivers and the impact (both in the short and long term) of mis/disinformation on civic space, and in particular on the enjoyment of fundamental freedoms, including the rights to freedom of peaceful assembly, of association and of expression.

Companies should:

36. Address the spread of mis/disinformation, including those derived from generative artificial intelligence that tries to delegitimize or manipulate facts related to peaceful protests and civil society, and refrain from arbitrarily removing posts or blocking pages linked to civil society and peaceful protests under the pretext of combating mis/disinformation. The use of artificial intelligence in content moderation must be compliant with due diligence and transparency obligation.

Online Hate Speech and Incitement to Violence

States should:

37. Condemn publicly and promptly, and effectively tackle the spread of hateful, misogynistic, and discriminatory online content, and cases of online incitement to hatred and violence against members of minority and marginalized communities, including civil society, activists, human rights defenders and journalists associated with these communities or working to promote and defend their rights;
38. Ensure that national hate speech legislation covers both offline and online hate speech and provides adequate and effective legal protection. In particular, ensure that law provides clear conditions for the removal of online hate speech as well as provides for effective investigations of hate speech punishable under the criminal law;
39. Ensure any legal or policy measures aimed at tackling hate speech, are in conformity with international human rights obligations, and in line with the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.⁶
40. Support measures to counter hate speech, such as through creating enabling environment for promoting free speech, through literacy and promoting alternative narratives aimed at fostering

⁶ See A/HRC/22/17/Add.4

intercultural understanding, equality, and respect for others; and enabling and facilitating broader public participation and debate.

41. Continue to implement the Rabat Plan of Action, among others, including through training and sensitizing security forces and law enforcement agents and those involved in the administration of justice, on issues concerning the prohibition of incitement to hatred, including online, and with respect to the rights to freedom of peaceful assembly and of association.
42. Refrain from sponsoring publicly or covertly online campaigns aimed at directly attacking or stigmatizing civil society and activists. Investigate and prosecute any such acts, including those committed by public officials, as well as by non-State actors.
43. Take measures to prevent and duly investigate and prosecute online abuse against women exercising their fundamental freedoms, which constitutes a direct attack on women's visibility and full participation in public life, and in turn undermines democracy.
44. Ensure that Internet platforms, such as social media, comply with their duties and responsibilities with respect to human rights, and to ensure that users do not disseminate speeches not protected by freedom of expression under the international human rights law.

Online platforms, including social media companies, should:

45. Ensure that their content moderation policies and practices with regard to hate speech are compliant with human rights standards, and ensure that such policies are transparent and publicly available;
46. Conduct human rights due diligence of their products, particularly assessing the role of algorithms and content recommender systems in amplifying hate speech and disinformation; and after public and meaningful consultation with all relevant stakeholders, adopt and make publicly available clear, transparent, narrowly defined policies on countering hate speech that are in line with international human rights law.

Artificial Intelligence (AI) Systems

States should:

47. Ensure, through policies and legislations, that human rights standards and safeguards are embedded throughout AI's entire lifecycle, from the design, development, deployment and use of the resulting models, tools and services, and retirement, as well as the collection and selection of data.
48. Adopt a comprehensive legal and ethical governance framework and regulations, as well as safeguards of the right to privacy, requiring assessment of the human rights risks and impacts of AI systems before, during, and after their use, including with regards to assembly and association rights.
49. Introduce transparency guarantees, independent oversight, and access to effective remedies, particularly when the State itself is using AI technologies.
50. Refrain from the use of facial recognition technologies and other biometric systems, to identify those peacefully participating in an assembly; and put in place a robust legal human rights-compliant regulatory framework that effectively protects the right to privacy, including with regards to facial images and the data derived from them.
51. Strictly regulate the use of AI, including facial recognition technologies and other biometric systems, to allow effective exercise of the rights to freedom of peaceful assembly, of association and of expression.

52. Establish effective, independent and impartial oversight mechanisms, with a regulatory power, for the use of biometrics, and impose a requirement of prior authorization and post-use review by an independent body for the use of such technologies in the context of assemblies.
53. Ban or suspend AI technologies that are posing unacceptable risk to human rights, including the rights to freedom of peaceful assembly, of association and of expression, until adequate safeguards are put in place. Ban facial recognition technologies that are used either for mass surveillance or discriminatory targeted surveillance.
54. Establish a moratorium on the use of facial recognition technologies in the context of peaceful assemblies, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards as well as safeguards against discrimination, and the rights to freedom of peaceful assembly, of association and expression.

Enabling and Supporting Digital Literacy

States should:

55. Address urgently digital literacy as a transversal measure to overcome the challenges identified in the previous sections of this joint declaration.
56. Encourage and invest in digital literacy education as a means to building resilience against misinformation /disinformation, online hate speech and incitement to violence, including counter-speech techniques.
57. Work to close the digital divide, including the gender digital divide, and secure an equitable and meaningful access to internet and online platforms for all, in order to increase the use of internet-based technologies as enablers and facilitators for public participation, and the enjoyment of the rights to freedom of peaceful assembly, of association and of expression.
58. As part of efforts to close the digital divide, enhance the access of women and girls to information and communications technologies, by promoting digital literacy and their participation in education and training on information and communications technologies, and by combatting persistent forms of gender-based discrimination and violence that prevent women and girls from enjoying equal access to, and equal participation in online fora and through the use of information and communications technologies.
59. Ensure safe online environment enabling civic action and public participation for all individuals and groups, including women, youth, LGBTI, indigenous groups, people with disabilities and other often marginalized and vulnerable communities.

Ensuring Effective Remedies and Accountability

States should:

60. Ensure that direct and indirect victims of human rights violations and abuses related to the use of digital technologies, including surveillance technologies, in the context of exercising their rights to freedom of peaceful assembly, of association and of expression online or offline, have effective access to justice and adequate reparations.
61. Ensure that law enforcement agencies are warned as to the potentially discriminatory impacts of certain policing tactics, including in the context of new technologies, and are trained to address them.
62. Investigate, identify, and hold accountable all State and non-State actors, responsible for cyber-attacks, online violence, threats and harassment, and the unlawful use of surveillance technologies, to target those exercising their rights to freedom of peaceful assembly, of association and expression

online and offline. Special efforts must be put towards identifying and prosecuting gender-based online violence and removing barriers preventing women from accessing justice.

63. Ensure those with authority are held responsible for abuses related to the unlawful use of surveillance and other AI technologies, targeting civil society, activists, human rights defenders, journalists and protesters.
64. Ensure transparent procurement policies and procedures that incorporate international human rights standards for the procurement of all digital technologies which are used by law enforcement, and other essential government public purposes.

Companies should:

65. Exercise systematic human rights due diligence to identify, prevent, mitigate and address violations of the rights to peaceful assembly, of association and expression.

The United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, Clément N. Voule

The Special Rapporteur on Human Rights Defenders and Focal Point for Reprisals in Africa of the African Commission on Human and Peoples' Rights (ACHPR), Rémy Ngoy Lumbu

The Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights (IACHR), Pedro Vaca Villareal

The Representative of Indonesia to the ASEAN Intergovernmental Commission on Human Rights (AICHR), Ms. Yuyun Wahyuningrum

The OSCE Office for Democratic Institutions and Human Rights (ODIHR)