WAVERING RESOLUTIONS: THE UN SECURITY COUNCIL ON DIGITAL RIGHTS

Digital, cyber, and human rights in the language of UN Security Council resolutions between 2001-2023

accessnow.org

accessnow

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

WAVERING RESOLUTIONS: THE UN SECURITY COUNCIL ON DIGITAL RIGHTS

Digital, cyber, and human rights in the language of UN Security Council resolutions between 2001-2023

June 2024

For more information, contact: UN@accessnow.org

Acknowledgements

This report is an Access Now publication, written by **Imène El Kadouri.**

The author would like to thank the Access Now team members who provided support, including Aymen Zaghdoudi, Giulio Coppi, Laura O'Brien, and Peter Micek.

Table of contents

Executive summary 3

Strong language for operations, peace, and security 5

Failure to name or confront cyber and digital threats to human rights 6

Positive developments amid inconsistency 8

Conclusion and recommendations 10

Annex: relevant language from General Assembly resolutions 13

Executive summary

The integration of digital and cyber matters into UN workstreams began more than 25 years ago,[1] and picked up steam over the past dozen years. As the UN Human Rights Council asserted in 2012,[2] and the UN General Assembly reaffirmed in 2024,[3] the same rights people enjoy offline must also be protected online.

In 2020, the UN Secretary General defined connectivity as "a foundation to ensure the continuation of critical services" and stated, "Inaccessibility to the Internet has posed a direct risk to individuals' ability to save their own lives and livelihoods, as well as for Governments and frontline workers to respond quickly and effectively" in the face of major crises.[4]

The international community in general, and the UN in particular, seems to agree on the importance of protecting and respecting human rights online and on the need for robust technology governance to maintain peace and security in the face of growing complexity and tensions. In 2023-2024, states battled in UN conference rooms over a landmark draft treaty on cybercrime,[5] digital surveillance in counter-terror efforts,[6] and the relevance of AI to international peace and security.[7]

Yet the digital dimension of our societies remains fraught and fragile. Despite its firm foundation in the International Bill of Rights, the legal framework surrounding human rights in the digital age remains patchy and inadequate. Even in the face of the impressive UN statements and work referenced above, some of the most important international bodies tasked with maintaining international peace and security have given digital rights only limited attention and protection.

In this brief, we set aside the assessment of gaps in digital governance in international law more generally, referring to existing research on this issue,[8] and focus specifically on the United Nations Security Council (UNSC), examining its language on digital age issues.

[1] See, e.g., https://disarmament.unoda.org/ict-security.
[2] In resolution A/HRC/20/L.13 : https://undocs.org/A/HRC/20/L.13
[3] In resolution A/78/L.49 : https://undocs.org/A/78/L.49
[4] https://www.un.org/en/content/digital-cooperation-roadmap/
[5] https://www.accessnow.org/guide/faq-un-cybercrime-convention-ahc/
[6] https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F77%2F298&Language=E&DeviceType=Desktop&LangRequested=False
[7] https://press.un.org/en/2023/sc15359.doc.htm
[8] See, e.g., https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf

Our analysis is based on a review of all UNSC resolutions adopted over the last three years (January 2020-January 2024, 218 resolutions), and a selection of relevant resolutions that the UNSC approved between 2001 and 2020 (122 resolutions).

The review focused on identifying language that refers to the digital and cyber dimensions of human rights and human security, and to the impact of digital-related events and systems on human rights, with the aim of better understanding the maturity of the integration of these concerns into the UNSC's work and documents.

We considered the explicit use of a non-exhaustive list of digital terms (e.g., "Internet," "data"), as well as more subtle or implicit language (e.g., "misinformation," "censorship," "access to services") when we deemed it relevant.

Our findings reveal a widening gap between the UNSC and other, more digitally aware, UN organs and bodies, when it comes to interpreting and including digital considerations related to human rights and security.

We highlight how the stronger UNSC language on digital and cyber issues that we identified tends to cover operational and physical security priorities rather than human rights concerns, and that most UNSC resolutions that actually name the cyber dimension of rights often lack accountability and protection components.

We conclude our review with a detailed set of recommendations for UNSC Member States. Broadly, we urge them to:

- **improve the language on digital and cyber issues connected to human rights**, especially when it comes to protection and accountability;
- **ensure consistency in expressions of concern regarding the impact of digital threats** affecting the safety, integrity, and security of UN missions and all civil society organizations and communities that are facing danger;
- **include** in any call to introduce digital solutions for peace and security **an adequately strong call to implement human rights due diligence and mitigation procedures**; and
- **expand the conceptual scope of "human security" to include digital and cyber aspects** that are today essential for such security.

Strong language for operations, peace, and security

The UNSC shows effective capacity to express and formalize concern for digital risks when these jeopardize the reputation, perception, and efficacy of UN work. Expression of this concern is also regularly accompanied by language calling for the introduction of new technologies or approaches that might mitigate those risks.

In particular, the precision and strength of the UNSC resolutions' language on digital risks when discussing UN peacekeeping missions is remarkable. Be it in regards to MINUSCA,[9] MINURSO,[10] UNIFIL,[11] MONUSCO, or UNMISS,[12] the UNSC has explicitly and repeatedly condemned disinformation, misinformation, and censorship campaigns against their work. The UNSC has also requested that the main actors involved, including the UN peacekeeping missions themselves and any relevant State, put in place strategies[13] to counter these threats.

The concern for security and safety is also evident in most resolutions related to threats to international peace and security caused by terrorist acts. When it comes to counterterrorism, UNSC resolution language has become more relevant to the digital age since 2001, reflecting broader digital and cyber developments. In particular, digital-focused language in UNSC resolutions evolved from broadly mentioning the "use of communications technologies by terrorist groups,"[14] to specify "various media, including the Internet"[15] or "biometric data"[16] and "social media."[17] Since then, the UNSC has continued to introduce more specific language in their periodic *Threats to international peace and security caused by terrorist acts* resolutions.[18]

---

[9] S/RES/2709 (2023): "*Demands that* ***all forms of violence against civilians, United Nations peacekeepers and humanitarian personnel, destabilising activities, incitement to hatred and violence, disinformation campaigns including through social media*** *[...] cease immediately"* (paragraph 3)
[10] S/RES/2703 (2023): *"Urges the parties and neighboring states to engage productively with MINURSO as it further considers how* ***new technologies*** *can be used to reduce risk, improve force protection, and better implement its mandate"* (paragraph 13)
[11] S/RES/2695 (2023): *"...condemns in the strongest terms "****disinformation campaigns*** *against UNIFIL"* (paragraph 15)
[12] S/RES/2677 (2023): *"...further condemning [...]* ***the harassment, targeting, and censorship of UNMISS"***
[13] S/RES/2695 (2023): "*requests UNIFIL [...] to strengthen its efforts to* ***monitor and to counter disinformation and misinformation*** *that might hinder the mission's ability to implement its mandate or threaten the safety and security of peacekeepers and to* ***develop an annual strategy to counter disinformation and misinformation***" (paragraph 23)
[14] S/RES/1373 (2001)
[15] S/RES/1617 (2005)
[16] S/RES/2161 (2014)
[17] S/RES/2170 (2014)
[18] See, e.g., S/RES/2178 (2014); S/RES/2322 (2016); S/RES/2396 (2017); S/RES/2610 (2021); S/RES/2617 (2021)

The language on digital risks in the fight against terrorism is also usually accompanied by reminders of the obligation to operate within the boundaries and guarantees set by human rights instruments.

Often, the UNSC also underlines the need for cooperation between States and private technology companies, and affirms the need for counterterrorism measures to respect "international human rights law, international refugee law, and international humanitarian law, underscoring that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures [...]."[19]

It is worth repeating, however, that the language the UNSC has chosen is limited to reminders of existing obligations under the current treaty system. The resolutions stop short of asking all interested parties to develop and put in place new mechanisms and strategies to prevent, mitigate, and counter human rights abuses.

We see a similar pattern when we look at the language for UNSC events and statements on Transnational Organized Crime (TOC), including cybercrime. Calls for deployment of digital tools and systems to combat cybercrime have increased over time, implying the UNSC sees these powerful new technologies as an unalloyed good, inherently harmless in nature.

These calls come with little to no evidence that the UNSC is taking into consideration the mission creep embedded in such systems[20] that often leads to mass surveillance and abuse, and no explicit recognition that communities and civil society organizations are often restricted from accessing secure technologies and further exposed to forms of TOC due to overbroad tech sanctions,[21] which force them to rely on alternative, unsecure, or unsupported solutions.

Failure to name or confront cyber and digital threats to human rights

Our analysis shows that there are differences among key UN policy-making organs and bodies when it comes to recognizing the digital and cyber dimensions of human rights and human security, or potential harms through digital means.

For example, the majority, if not all, of the human rights-related resolutions in the UN General Assembly and Human Rights Council promote and protect the rights to freedom of

[19] S/RES/2178 (2014)
[20] See, e.g., Access Now, *Mapping Humanitarian Tech* (2024) https://www.accessnow.org/mapping-humanitarian-tech
[21] See, e.g., Access Now "When sanctions undermine human rights online" (2023) https://www.accessnow.org/sanctions-undermining-human-rights/

expression, peaceful assembly, and privacy. They each address topics that are relevant to protecting these rights, including the safety of journalists and media professionals, data protection, encryption and anonymity, digital divides, and the need to condemn all forms of hate speech, harassment, and censorship of civil society.

The Human Rights Council has spearheaded the recognition of digital rights at the UN. Since 2012, it has led various iterations of the resolution on *the promotion, protection and enjoyment of human rights on the Internet*, addressing digital topics through a human rights perspective. More recently, the General Assembly followed suit. In 2023, it passed — by consensus — a resolution on *the promotion and protection of human rights in the context of digital technologies*.[22] This may be the first time the General Assembly has advanced a comprehensive dedicated resolution to address digital technologies from a human rights perspective, but there are signs we will see more activity in this area.

In early 2024, the United States — a permanent member of the UNSC — chose to propose a resolution on artificial intelligence within the General Assembly,[23] not the UNSC. This choice confirms what we see in our analysis: the UNSC is lagging behind the Human Rights Council and General Assembly in integrating the digital perspective on human rights harms and risks.

The UNSC's persistent failure to mention the digital systems and platforms where security and safety risks and threats either thrive, or are suppressed,[24] leaves obvious gaps that come at a significant cost to human security. These gaps speak of a lack of recognition that today, we must address the human rights challenges of the digital age from a multistakeholder perspective, especially in contexts where people are facing violence and conflict.

The UNSC has shown that it is aware of the seriousness and urgency of these threats. In some instances, it has tackled digital challenges such as access to telecommunication,[25] incitement

---

[22] A/RES/78/213

[23] On March 14, a Joint Statement on the Proposed UNGA Resolution on Artificial Intelligence Systems for Sustainable Development was published stating that "The text also establishes a shared vision that AI systems should be human-centric, reliable, explainable, ethical, inclusive, privacy preserving, and responsible, with a sustainable development orientation, and in full respect, promotion and protection of human rights and international law. See more: https://usun.usmission.gov/joint-statement-on-the-proposed-unga-resolution-on-seizing-the-opportunities-of-safe-secure-and-trustworthy-ai-systems-for-sustainable-development/

[24] See e.g., *"strongly encouraging all parties to **create a safe and enabling environment for members of civil society, including those who promote and protect human rights**, to carry out their work independently and without undue interference, including in situations of armed conflict, and to address threats, harassment and violence, to **counter hate speech against them, and to protect and promote human rights and fundamental freedoms, including freedom of expression, peaceful assembly and association**, in accordance with obligations under international law, to help enable free, fair, transparent and inclusive elections and national reconciliation"* (S/RES/2702)

[25] See, e.g., S/RES/2720 (2023), "The situation in the Middle East, including the Palestinian question"

to hatred and violence on social media platforms,[26] or data collection,[27] sometimes even showing a clear capacity to adopt effective and poignant language.

However, it has for the most part demonstrated a disconnect between awareness of the problem and formal recognition. For example, during the discussion on the 2021 UNSC *Protection of civilians in armed conflict* resolution,[28] many Member States vehemently highlighted the gravity of targeting civilian infrastructure and violating human rights through cyber means in their oral statements,[29] yet this element of the threat was not captured in the final text.

Positive developments amid inconsistency

As we note above, the UNSC has produced good digital rights language. In the latest *Maintenance of peace and international security* resolution,[30] for example, the UNSC not only "expresses deep concern at instances of violence fuelled by hate speech, misinformation and disinformation, including through social media platforms," but also recognizes "the importance of [...] media online as well as offline, including Internet-based platforms such as social media [...] in promoting tolerance and peaceful coexistence" as well as encouraging "all stakeholders, including [...] media entities and social media platforms to speak out against hate speech."

But the UNSC does not adopt this tone consistently, and most resolutions only contain brief mentions of digital aspects of human rights (if any at all). For instance, while the above-referenced resolution on the situation in the Democratic Republic of Congo[31] explicitly acknowledges the harmful effects of misinformation and disinformation on social media platforms, the digital-related language in the resolution on Myanmar[32] mentions only the "restrictions on medical personnel, civil society, labor union members, journalists and media workers," ignoring the overwhelming evidence of censorship and online disinformation campaigns, and the documented harmful impact misinformation, disinformation, and hate speech have had in the country.

---

[26] See, e.g., S/RES/2709 (2023), "The situation in the Central African Republic (MINUSCA)"
[27] See, e.g., S/RES/2331 (2016), *"Maintenance of international peace and security," "requests further that the Secretary-General takes steps to improve the collection of data, monitoring and analysis of trafficking in persons in the context of armed conflict, in order to better identify and prevent its incidence"*
[28] S/RES/2573 (2021)
[29] Security Council Strongly Condemns Attacks against Critical Civilian Infrastructure, Unanimously Adopting Resolution 2573 (2021), UN Press release, https://press.un.org/en/2021/sc14506.doc.htm
[30] S/RES/2686 (2023)
[31] *"...remaining deeply concerned by [...] "the intensification of intercommunal violence fuelled by hate speech, misinformation and disinformation, including through social media platforms"* S/RES/2717 (2023)
[32] S/RES/2669 (2022)

Similarly, one of the first resolutions regarding the most recent humanitarian crisis in Gaza and the impact of the military operations led by Israel[33] *recognizes* the need for the civilian population in the Gaza strip to have access to electricity and telecommunications, a very important and positive point. However, at the same time, the resolution does not mention the series of Internet shutdowns the population has been experiencing, nor does it address the military attacks on civilian telecommunications infrastructure and their devastating impacts for civilians.[34] The resolution also fails to expressly demand the return of connectivity, specify who should ensure access, offer a timetable for implementation and review, or commit resources to restoration.

Even in its resolutions on UN peacekeeping mission review or renewal, the UNSC ignores the risks to the population, despite including relatively stronger language on countering cyber attacks, campaigns, and interferences. The mandate and protection of civilians (PoC) frameworks do not adequately consider the digital dimension of threats against civilians, nor do they provide guidance on managing such risks. The 2019 and 2023 DPO Policy on PoC in Peacekeeping[35] specifies that missions may protect individuals "in cases of credible threats of physical violence," but fails to consider that such threats and their impact are increasingly generated or amplified through digital systems. There is information on some of these concerns in the UN Peacemaker's (DPPA) Digital Technologies and Mediation Toolkit, leaving hope that the UNSC will include more formal consideration of the digital component in DPPA policies in the future.[36]

Similarly, even though UNSC resolutions often underscore the need for free and fair elections, or highlight tense or delicate democratic processes, they do not mention the importance of protecting access to Internet and communications systems, which is essential for ensuring full and free participation by everyone. These omissions point to the UNSC's lack of appreciation for the fact that civic space and public debate have incrementally shifted to online platforms.

[33] S/RES/2720 (2023)
[34] Palestine unplugged: how Israel disrupts Gaza's internet (2023). Access Now report. https://www.accessnow.org/publication/palestine-unplugged/
[35] DPO Policy on PoC in Peacekeeping (2023). UN Policy. https://peacekeeping.un.org/sites/default/files/2023_protection_of_civilians_policy.pdf
[36] https://peacemaker.un.org/digitaltoolkit

Conclusion and recommendations

Our analysis reveals a troubling lack of willingness in the UNSC to recognize how much the full enjoyment of human rights and security is intertwined and dependent on our shared digital ecosystem.

UNSC resolutions also fail to address the impact of cyber and digital surveillance and Internet service disruption on already vulnerable communities, or the risks posed by the technologies and systems that some UN peacekeeping missions are using.

In short, the UNSC is overlooking the overall advancement of international law protecting people, peace, and security in the digital age, focusing on operational and physical security at the expense of human rights and human security.

When the UNSC addresses digital issues (e.g. content governance, surveillance technology, data collection, freedom of expression, social media platforms, censorship, access to telecommunications, online propaganda, modern technologies), it does so *without* the lens of accountability and protection of human rights.

Many of these gaps may be due to underinvestment by UNSC Member States in their diplomatic corps, who may lack adequate knowledge of digital and cyber issues. The quick pace of regional and global crises creates a heavy workload that, especially for states with fewer personnel in their UN Missions, could push new and emerging technologies off the priority list. Adopting a more robust approach to human security in the digital age will entail staffing up and engaging more deeply with affected communities, NGOs, academics, and private-sector experts.

The diplomatic corps can also draw important lessons from the work done by the UN General Assembly. For example, the UNSC could include language on the importance of an accessible, inclusive, and safe digital environment for persons in vulnerable situations and a call to refrain from “undue restrictions, such as Internet shutdowns, arbitrary or unlawful surveillance or online censorship” (see Annex, A/RES/78/213) in its resolutions on volatile countries or regions (e.g. Ukraine, Gaza, Sudan), as well as in thematic resolutions. The same A/RES/78/213 from the General Assembly could inform existing UNSC thematic resolutions on issues such as “Protection of civilians in armed conflict,” “Threats to international peace and security caused by terrorist acts,” and “Maintenance of international peace and security,” reaffirming the primacy of the rights-based approach in tackling the greatest challenges and threats facing humanity.

In A/RES/78/213, the General Assembly does not hesitate to reiterate "that all human rights are universal, indivisible, interrelated, interdependent and mutually reinforcing, and affirming that the same rights that people have offline must also be protected online," and it recognizes "the need to ensure that human rights are promoted, respected, protected and fulfilled through the entirety of digital technologies' life cycle." The General Assembly also notes the risks emerging from new, unregulated digital technologies that impact the enjoyment of human rights and recognizes "the need for prevention, remedy, and accountability measures and recalled the obligations of States and responsibilities of business enterprises."[37] Examples like this are plentiful, and with human rights and security at stake, there is no excuse to ignore them.

As the UNSC continues its deafening silence on these issues, states and armed parties are getting bolder in weaponizing existing communication networks, and in suppressing opposing voices or blocking the use of alternative information systems altogether. Communities and their advocates are left to fend for themselves in reclaiming safe and unhindered access to the Internet and telecommunications, in demanding protection when voicing their concerns or raising their opinions online, and in opposing intrusive and abusive surveillance technologies.

We recommend that UNSC Member States:

- Map the intersection of their signature issues with human rights and security in the digital age, review their current capacity on digital and cyber issues, and seek to introduce these aspects into UNSC resolutions and debates, in close coordination with affected communities and non-governmental organizations and experts;
- When referring to the protection of civilians, introduce, adapt, and create consensus on existing UNSC language on digital issues, currently used for operational security or countering terrorism, and frame it instead through the lens of accountability and protection of civilians;
- Take inspiration from the work already carried out by the UN General Assembly in recognizing the challenges to human rights in the digital age, and repurpose

[37] A/RES/78/213: *"uses of **new and emerging digital technologies that impact the enjoyment of human rights may lack adequate regulation and governance mechanisms**," "recognizes the **need for accountability and effective measures to prevent, mitigate and remedy potential and actual adverse human rights impacts** of such technologies **in line with obligations of States under international human rights law and responsibilities of business enterprises in line with the Guiding Principles on Business and Human Rights**."*

some of the adopted language (see examples above, and full list in the Annex below);

- Extend the same concern for the safety, efficiency, performance, and reputation of UN activities and peace operations both in digital and physical spaces, and to civilians, civil society, and humanitarian organizations alike, when tackling issues such as spyware/surveillance, disinformation/misinformation, or hate speech; and
- Include in all UNSC resolutions that call for the introduction or strengthening of technological, and especially digital, solutions for peace and security purposes, the demand that mechanisms, strategies, and procedures be put in place to protect human rights and mitigate possible harmful impacts, in the strongest terms possible.

In addition, the UNSC as a body should:

- Encourage states to promote an understanding of "human security" as necessarily including secure and open access to the Internet, and to strengthen protections for Internet access during armed conflict (protecting the digital lifeline); language on digital rights can be found in a variety of instruments, such as international human rights law (IHRL), international humanitarian law (IHL), and other international frameworks, none of which currently function to provide adequate protections during armed conflict.

Annex: relevant language from General Assembly resolutions

A/RES/73/173 - Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association

- 4. Calls upon all States to ensure that the same rights that individuals have offline, including the rights to freedom of expression, of peaceful assembly and of association, are also fully protected online, in accordance with human rights law, particularly by refraining from **Internet shutdowns and content restrictions on the Internet that violate international human rights law, by ending attacks by States and taking steps to end attacks by non-State actors against journalists and other media workers covering demonstrations and protests and by ending government shutdowns of media outlets for attempting to report on such protests**, and condemns unequivocally and calls for an end to all attacks and violence by State and non-State actors against journalists and media workers, including through attacks on, or the forced closure of, their offices and media outlets, in both conflict and non-conflict situations, in particular for journalists and media outlets covering or attempting to cover demonstrations and protests

A/RES/74/173 - Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing

- Stressing the need to enhance coordination and cooperation among Member States in combating cybercrime, including by providing technical assistance to developing countries, upon request, to improve national legislation and enhance the capacity of national authorities to deal with cybercrime in all its forms, including its prevention, detection, investigation, and prosecution, emphasizing in this context the role that the United Nations, in particular the Commission on Crime Prevention and Criminal Justice, plays, and **reaffirming the importance of respect for human rights and fundamental freedoms in the use of information and communication technologies**
- 5. Encourages Member States to develop and implement measures to ensure that cybercrime and crimes in which electronic evidence is relevant can be effectively investigated and prosecuted at the national level and that effective international cooperation can be obtained in this area, **in accordance with domestic law and consistent with relevant and applicable international law, including applicable international human rights instruments**

A/RES/76/227 - Countering disinformation for the promotion and protection of human rights and fundamental freedoms

- Stressing that responses to the spread of disinformation must comply with **international human rights law and the principles of legality, necessity, and proportionality, and underlining the importance of free, independent, plural, and diverse media and of providing and promoting access to independent, factual, and evidence-based information to counter disinformation**
- Reaffirming the need to ensure that efforts to counter disinformation promote and protect and **do not violate individuals' freedom of expression and freedom to seek, receive, and impart information**, and noting that media and information-related technology literacy can help to achieve this through independent and free media, awareness-raising, and a focus on the empowerment of people
- Encouraging States, international and regional organizations, national human rights institutions and civil society, business enterprises, including media, online platforms, social media, and technology companies, to **foster respect for human rights online and offline** in the context of new and emerging digital technologies and human rights due diligence processes
- 1. Emphasizes that all forms of disinformation can **negatively impact the enjoyment of human rights and fundamental freedoms**, as well as the attainment of the Sustainable Development Goals
- 6. Expresses concern about the spread of disinformation and propaganda, including on the Internet, which can be designed and implemented so as to mislead, to **violate human rights, including the rights to privacy and to freedom of expression**, to spread hatred, racism, xenophobia, negative stereotyping or stigmatization, and to incite violence, discrimination and hostility, and emphasizes the important contribution by journalists in countering this trend
- 11. Encourages online platforms, including social media companies, to review their business models and ensure that their design and development processes, their business operations, data collection and data processing practices are in line with **the Guiding Principles on Business and Human Rights, and emphasizes the importance of conducting human rights due diligence** of their products, particularly of the role of algorithms and ranking systems in amplifying disinformation, and calls upon them to adopt and make publicly available, after consultation with all relevant stakeholders, clear, transparent, narrowly defined content and advertising policies on countering disinformation that are in line with international human rights law
- 13. Underlines that countering disinformation requires multidimensional and multi-stakeholder responses that are **in compliance with international human rights**

law and the proactive engagement of international organizations, States, business enterprises, and all other stakeholders

- 15. Invites the Office of the United Nations High Commissioner for Human Rights, special procedures, treaty bodies, and all other human rights mechanisms and entities of the United Nations, within their respective mandates, to consider, as appropriate, addressing **the impact of disinformation on human rights**

A/RES/75/176 - The right to privacy in the digital age

- Noting that the rapid pace of technological development enables individuals all over the world to use new information and communications technologies, and at the same time enhances the capacity of Governments, business enterprises, and individuals to undertake surveillance, interception, and data collection, which may **violate or abuse human rights, in particular the right to privacy**, as set out in **Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights**, and is therefore an issue of increasing concern
- Reaffirming **the human right to privacy**, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, and the right to the protection of the law against such interference, and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society
- Recognizing the need to further discuss and analyze, based on **international human rights law**, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, **the impact of surveillance on the right to privacy and other human rights**, as well as the need to examine the principles of non-arbitrariness, lawfulness, legality, necessity, and proportionality in relation to surveillance practices,
- Noting also that the use of artificial intelligence can contribute to **the promotion and protection of human rights** and has the potential to transform governments and societies, economic sectors, and the world of work and can also have various far reaching implications, including with regard to the right to privacy
- Expressing concern about the spread of disinformation and misinformation, particularly on **social media platforms**, which can be designed and implemented so as to mislead, to spread racism, xenophobia, negative stereotyping, and

stigmatization, **to violate and abuse human rights,** including the right to privacy, to impede freedom of expression, including the freedom to seek, receive, and impart information, and to incite all forms of violence, hatred, intolerance, discrimination, and hostility, and emphasizing the important contribution of journalists, civil society, and academia in countering this trend

- Emphasizing that **States must respect international human rights obligations regarding the right to privacy** when they intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information- and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including business enterprises

A/RES/78/213 - Promotion & protection of human rights in the context of digital technologies

- Reiterating that all human rights are universal, indivisible, interrelated, interdependent and mutually reinforcing, and affirming that **the same rights that people have offline must also be protected online**
- Noting that **the increasing use of digital technologies has impacts on the enjoyment of a wide range of human rights**, and recognizing that **digital technologies can work as enablers of human rights, but that, without appropriate safeguards, they can be used to seriously threaten the protection and full enjoyment of human rights**
- Recognizing **the need to ensure that human rights are promoted, respected, protected, and fulfilled through the entirety of digital technologies' life cycle**, including through their conception, design, development, deployment, use, evaluation, and regulation, and to ensure that they are subject to adequate safeguards in order to promote a free, open, universal, interoperable, safe, secure, stable, accessible, and affordable **digital environment for all**
- Recognizing also that **certain applications of new and emerging digital technologies are not compatible with international human rights law**, and noting that uses of new and emerging digital technologies that impact the enjoyment of human rights may **lack adequate regulation and governance mechanisms**, and recognizing the **need for accountability and effective measures** to prevent, mitigate, and remedy potential and actual adverse human rights impacts of such technologies in line with obligations of States under international human rights law and responsibilities of business enterprises in line with the Guiding Principles on Business and Human Rights

- Recognizing further that a lack of access to affordable, safe, quality, and reliable technologies and services remains **a critical challenge in many developing countries**
- Stressing the importance for all Member States, and stakeholders as appropriate, to promote universal, free, open, interoperable, safe, reliable, and secure use of and access to the Internet by facilitating international cooperation aimed at the development of media and information and communications facilities in all countries, by respecting and protecting human rights and by **refraining from undue restrictions, such as Internet shutdowns, arbitrary or unlawful surveillance, or online censorship**
- Underlining that digital contexts provide opportunities for exercising human rights, including by improving access to information, and by seeking, receiving, and imparting information and ideas of all kinds, and emphasizing that efforts to promote access to digital technologies, digital, media and information literacy, civic participation, and online safety are important to bridge digital divides and ensure digital inclusion in its broader interpretation, which includes the development of digital skills
- Noting with deep concern the use of technological tools developed by the private surveillance industry and by private or public actors to undertake **surveillance, hacking of devices and systems, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defense of human rights and fundamental freedoms, journalists, and other media workers, in violation or abuse of their human rights**
- Noting that the use of **algorithmic or automated decision-making processes can negatively affect the enjoyment of human rights**, including by perpetuating stereotypes or by resulting in discrimination, in particular when the data used for the training of algorithms are non-representative, inaccurate, or irrelevant
- Noting with concern that **artificial intelligence or machine-learning technologies, without human rights safeguards, as well as proper technical, regulatory, legal, and ethical safeguards, and without adequate and effective evaluation and feedback mechanisms, may pose the risk** of reinforcing systemic, racial, and gender-based discrimination and can lead to decisions that have the potential to affect the enjoyment of human rights, including economic, social, and cultural rights, and affect non-discrimination, and recognizing the need to prevent racial and otherwise discriminatory outcomes and apply international human rights law and data-protection frameworks in the conception, design, development, deployment, use, evaluation, and regulation of these technologies and practices

- Recognizing that **persons in vulnerable situations, including children, may be particularly exposed to online risks**, and that there is a need to take steps to ensure that the digital environment, including safety information, protective strategies, services, and forums relating to it, is accessible, inclusive, and safe
- 3. Calls upon all Member States: (a) To consider developing or maintaining and implementing adequate legislation, **in consultation with all relevant stakeholders, including business enterprises, international organizations, civil society, and technical and academic communities**, with effective sanctions and appropriate remedies, that protects individuals against violations and abuses of their human rights in the digital context
- 6. Calls upon **the private sector and all relevant stakeholders to ensure that respect for human rights is incorporated** into the conception, design, development, deployment, operation, use, evaluation, and regulation of all new and emerging digital technologies and to provide for redress and effective remedy for the human rights abuses that they may cause, contribute to, or to which they may be directly linked

A/78/L.49 - Seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development

- Recognizing also that the improper or malicious design, development, deployment, and use of artificial intelligence systems, such as without adequate safeguards or in a manner inconsistent with international law, pose risks that could hinder progress towards the achievement of the 2030 Agenda for Sustainable Development and its Sustainable Development Goals, and **undermine sustainable development in its three dimensions – economic, social, and environmental; widen digital divides between and within countries; reinforce structural inequalities and biases; lead to discrimination; undermine information integrity and access to information; undercut the protection, promotion, and enjoyment of human rights and fundamental freedoms, including the right not to be subject to unlawful or arbitrary interference with one's privacy; and increase the potential risk for accidents and compound threats from malicious actors**
- 5. Emphasizes that human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems, calls upon all Member States and, where applicable, other stakeholders to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the

enjoyment of human rights, especially of those who are in vulnerable situations, and reaffirms that **the same rights that people have offline must also be protected online**, including throughout the life cycle of artificial intelligence systems

- 6. Encourages all Member States, where appropriate, in line with their national priorities and circumstances and while implementing their distinct national regulatory and governance approaches and frameworks, and, where applicable, other stakeholders to promote safe, secure, and trustworthy artificial intelligence systems in **an inclusive and equitable manner, and for the benefit of all, and foster an enabling environment for such systems to address the world's greatest challenges, including achieving sustainable development in its three dimensions – economic, social and environmental – with specific consideration of developing countries and leaving no one behind** [...]