

**Seventy-seventh session**

Agenda item 68 (b)

Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms**Resolution adopted by the General Assembly
on 15 December 2022***[on the report of the Third Committee (A/77/463/Add.2, para. 87)]***77/211. The right to privacy in the digital age***The General Assembly,*

Reaffirming the purposes and principles of the Charter of the United Nations, the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights¹ and relevant international human rights treaties, including the International Covenant on Civil and Political Rights² and the International Covenant on Economic, Social and Cultural Rights,³ as well as the Vienna Declaration and Programme of Action,⁴

Recalling General Assembly resolutions [68/167](#) of 18 December 2013, [69/166](#) of 18 December 2014, [71/199](#) of 19 December 2016, [73/179](#) of 17 December 2018 and [75/176](#) of 16 December 2020 on the right to privacy in the digital age, and resolution [45/95](#) of 14 December 1990 on guidelines for the regulation of computerized personal data files, as well as Human Rights Council resolutions [28/16](#) of 26 March 2015,⁵ [34/7](#) of 23 March 2017,⁶ [37/2](#) of 22 March 2018,⁷ [42/15](#) of 26 September 2019⁸ and [48/4](#) of 7 October 2021⁹ on the right to privacy in the digital

¹ Resolution [217 A \(III\)](#).

² See resolution [2200 A \(XXI\)](#), annex.

³ *Ibid.*

⁴ [A/CONF.157/24 \(Part I\)](#), chap. III.

⁵ See *Official Records of the General Assembly, Seventieth Session, Supplement No. 53 (A/70/53)*, chap. III, sect. A.

⁶ *Ibid.*, *Seventy-second Session, Supplement No. 53 (A/72/53)*, chap. IV, sect. A.

⁷ *Ibid.*, *Seventy-third Session, Supplement No. 53 (A/73/53)*, chap. IV, sect. A.

⁸ *Ibid.*, *Seventy-fourth Session, Supplement No. 53A (A/74/53/Add.1)*, chap. III.

⁹ *Ibid.*, *Seventy-sixth Session, Supplement No. 53A (A/76/53/Add.1)*, chap. IV, sect. A.



age and resolutions [32/13](#) of 1 July 2016¹⁰ and [38/7](#) of 5 July 2018¹¹ on the promotion, protection and enjoyment of human rights on the Internet,

Recalling also the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society,¹²

Taking note of the reports of the Special Rapporteur of the Human Rights Council on the right to privacy,¹³ the reports of the Special Rapporteur of the Human Rights Council on the promotion and protection of the right to freedom of opinion and expression¹⁴ and the relevant reports of the Special Rapporteur of the Human Rights Council on the rights to freedom of peaceful assembly and of association,¹⁵ as well as the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance,¹⁶

Welcoming the work of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, noting with interest the reports of the High Commissioner thereon,¹⁷ and recalling the expert workshops on the right to privacy in the digital age held on 19 and 20 February 2018 and on 27 and 28 May 2020,

Taking note of the Secretary-General's strategy on new technologies and his Road Map for Digital Cooperation,¹⁸ and noting the discussions that take place annually in the Internet Governance Forum, which is a multi-stakeholder forum for the discussion of Internet governance issues and whose mandate was extended by the General Assembly in 2015 for another 10 years, and recognizing that effectively addressing the challenges relating to the right to privacy in the context of modern communications technology requires an ongoing, concerted multi-stakeholder engagement,

Noting that the rapid pace of technological development enables individuals all over the world to use new information and communications technologies that empower people, improve lives, strengthen justice and boost productivity, and at the same time enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception, hacking 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,

Noting also that violations and abuses of the right to privacy in the digital age can affect all individuals, with particular effects on women, children, in particular girls, persons with disabilities and older persons, as well as those in vulnerable situations,

Recognizing that new and emerging digital technologies, in particular assistive digital technologies, can especially contribute to the full enjoyment of human rights by persons with disabilities, and that these technologies should be designed in consultation with them and with appropriate safeguards to protect their rights, including their right to privacy,

¹⁰ Ibid., *Seventy-first Session, Supplement No. 53 (A/71/53)*, chap. V, sect. A.

¹¹ Ibid., *Seventy-third Session, Supplement No. 53 (A/73/53)*, chap. VI, sect. A.

¹² Resolution [70/125](#).

¹³ [A/HRC/43/52](#), [A/HRC/46/37](#), [A/HRC/49/55](#), [A/75/147](#) and [A/76/220](#).

¹⁴ [A/HRC/44/49](#), [A/HRC/50/29](#), [A/75/261](#) and [A/76/258](#).

¹⁵ [A/HRC/44/50](#), [A/HRC/50/23](#), [A/HRC/50/42](#) and [A/75/184](#).

¹⁶ [A/HRC/44/57](#), [A/75/329](#) and [A/76/434](#).

¹⁷ [A/HRC/48/31](#) and [A/HRC/51/17](#).

¹⁸ [A/74/821](#).

Recognizing also that the promotion of and respect for the right to privacy are important to the prevention of violence, including gender-based violence, abuse and sexual harassment, in particular against women and children, as well as any form of discrimination, which can occur in digital and online spaces and includes cyberbullying and cyberstalking,

Noting that children can be particularly vulnerable to abuses and violations of their right to privacy,

Noting also that States parties should implement the Convention on the Rights of the Child¹⁹ in relation to the digital environment, including the importance of privacy to children's agency, dignity and safety, and for the exercise of their rights,

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,

Recalling with appreciation general comment No. 16 of the Human Rights Committee on article 17 of the International Covenant on Civil and Political Rights, on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation,²⁰ while also noting the vast technological leaps that have taken place since its adoption and the need to discuss the right to privacy in view of the challenges of the digital age,

Recognizing the need to further discuss and analyse, 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,

Recognizing also that the discussion on the right to privacy should be based upon existing international and domestic legal obligations, including international human rights law, as well as relevant commitments, and should not open the path for undue interference with an individual's human rights,

Recognizing further the need to ensure that international human rights obligations are respected in the conception, design, development, deployment, evaluation and regulation of data-driven technologies and to ensure that they are subject to adequate safeguards and oversight,

Stressing the importance of full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation,

Recognizing that the right to privacy is important for the enjoyment of other rights and can contribute to an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to be free from unlawful or arbitrary interference with the right to privacy might affect the enjoyment of other human rights, including the right to freedom of

¹⁹ United Nations, *Treaty Series*, vol. 1577, No. 27531.

²⁰ *Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40)*, annex VI.

expression and to hold opinions without interference, and the right to peaceful assembly and freedom of association,

Noting that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity,

Expressing concern that individuals, particularly children, often do not and/or cannot provide their free, explicit and informed consent to the collection, processing and storage of their data or to the reuse, sale or multiple resale of their personal data, as the collection, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age,

Noting that general comment No. 16 of the Human Rights Committee recommends that States take effective measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises,

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,

Noting with concern that artificial intelligence or machine-learning technologies, without proper technical, regulatory, legal and ethical safeguards, may 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 apply international human rights law and data protection frameworks in the design, evaluation and regulation of these practices,

Recognizing that, while the use of artificial intelligence can have significant positive economic and social impacts, it requires and allows for the processing of large amounts of data, often relating to personal data, including biometric data and data on an individual's behaviour, social relationships, race or ethnicity, religion or belief, which can pose serious risks to the enjoyment of the right to privacy, especially when done without proper safeguards, in particular when employed for identification, tracking, profiling, facial recognition, classification, behaviour prediction or scoring of individuals,

Noting that the use of artificial intelligence may, without proper technical, regulatory, legal and ethical safeguards, pose the risk of reinforcing discrimination, including structural inequalities, and recognizing that racially and otherwise discriminatory outcomes should be prevented in the design, development, implementation and use of emerging digital technologies,

Noting with concern that certain predictive algorithms are likely to result in discrimination, including when non-representative data are used,

Noting that the use of algorithmic or automated decision-making processes online can affect the enjoyment of individuals' rights offline,

Noting also that the use of data extraction and algorithms to target content towards online users may undermine user agency and access to information online, as well as the right to freedom of opinion and expression,

Noting with concern reports indicating lower accuracy of facial recognition technologies with certain groups, including when non-representative training data are used, that the use of digital technologies can exacerbate racial inequality and in this context the importance of effective remedies,

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and to hold opinions without interference, the right to freedom of peaceful assembly and association and the right to freedom of religion or belief and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale,

Recognizing that the same rights that people have offline must also be protected online, including the right to privacy,

Noting that the accelerated synchronization of online and offline spaces can affect individuals' enjoyment of their human rights, including their right to privacy,

Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant,

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,

Noting with deep concern that, in many countries, persons and organizations engaged in promoting and defending human rights and fundamental freedoms, journalists and other media workers may frequently face threats and harassment and suffer insecurity, as well as unlawful or arbitrary interference with their right to privacy, as a result of their activities,

Noting with deep concern also 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 defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights, specifically the right to privacy,

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,

Noting the increase in the collection of sensitive biometric information from individuals, and stressing that States must comply with their human rights obligations and that business enterprises should respect the right to privacy and other human

rights when collecting, processing, sharing and storing biometric information by, inter alia, adopting data protection policies and safeguards,

Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights,

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications and transactions, including measures for strong encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and recognizing that States should promote such measures and refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking,

Noting that, while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law,

Noting also, in that respect, that the prevention and suppression of terrorism is a public interest of great importance, while reaffirming that States must ensure that any measures taken to combat terrorism are in compliance with their obligations under international law, in particular international human rights, refugee and humanitarian law,

Recognizing that a lack of access to affordable and reliable technologies and services remains a critical challenge in many developing countries,

Stressing the need to address prevailing challenges to bridge the digital divides, both between and within countries, and the gender digital divide, and to harness information and communications technologies for development, and recalling the need to emphasize quality of access to bridge digital and knowledge divides, using a multidimensional approach that includes speed, stability, affordability, language, training, capacity-building, local content and accessibility for persons with disabilities, and to promote the full enjoyment of human rights, including the right to privacy,

Stressing also the need to ensure that national security and public health measures, including the use of technology to monitor and contain the spread of infectious diseases, are in full compliance with the obligations of States under international human rights law and adhere to the principles of lawfulness, legality, legitimacy with regard to the aim pursued, necessity and proportionality and the need to protect human rights, including the right to privacy, and personal data in the response to health or other emergencies,

Noting the importance of protecting and respecting the right of individuals to privacy when designing, developing or deploying technological means in response to disasters, epidemics and pandemics, especially the coronavirus disease (COVID-19) pandemic, including digital exposure notification and contact tracing,

Noting also that new and emerging digital technologies can contribute to the recovery from global health emergencies, including the COVID-19 pandemic, and recalling in this regard the importance of protecting human health-related and other personal data, while noting with concern that some efforts to combat the COVID-19 pandemic have an adverse impact on the enjoyment of the right to privacy,

1. *Reaffirms* the 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,

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;

2. *Recognizes* the global and open nature of the Internet and the rapid advancement in information and communications technologies as a driving force in accelerating progress towards development in its various forms, including in achieving the Sustainable Development Goals;²¹

3. *Affirms* that the same rights that people have offline must also be protected online, including the right to privacy, with special regard given to the protection of children;

4. *Recalls* that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality;

5. *Encourages* all States to promote an open, secure, stable, accessible and peaceful information and communications technology environment based on respect for international law, including the obligations enshrined in the Charter of the United Nations and human rights instruments;

6. *Acknowledges* that the conception, design, use, deployment and further development of new and emerging technologies, such as those that involve artificial intelligence, may have an impact on the enjoyment of the right to privacy and other human rights, and that the risks to these rights can and should be avoided and minimized by adapting or adopting adequate regulation or other appropriate mechanisms, in accordance with applicable obligations under international human rights law, for the conception, design, development and deployment of new and emerging technologies, including artificial intelligence, by taking measures to ensure a safe, transparent, accountable, secure and high quality data infrastructure and by developing human rights-based auditing mechanisms and redress mechanisms and establishing human oversight;

7. *Calls upon* all States:

(a) To respect and protect the right to privacy, both online and offline, including in the context of digital communications and new and emerging technologies;

(b) To invite all relevant stakeholders to further discuss how emerging phenomena, such as the push for widespread adoption of blockchain, expanded and virtual reality technologies and the development of increasingly powerful neurotechnology, without proper safeguards, have an impact on the enjoyment of the right to privacy and the right to freedom of opinion and expression;

(c) To take measures to put an end to violations of the right to privacy and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(d) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

²¹ See resolution [70/1](#).

(e) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

(f) To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations;

(g) To consider developing or maintaining and implementing adequate legislation, in consultation with all relevant stakeholders, including business enterprises, international organizations and civil society, with effective sanctions and appropriate remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention, sharing or use of personal data by individuals, Governments, business enterprises and private organizations;

(h) To consider developing or maintaining and implementing legislation, regulations and policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully respect the right to privacy and other relevant human rights in the design, development, deployment and evaluation of technologies, including artificial intelligence, and to provide individuals whose rights may have been violated or abused with access to an effective remedy, including compensation and guarantees of non-repetition;

(i) To consider adopting or maintaining data protection legislation, regulation and policies, including on digital communication data, that comply with their international human rights obligations, which could include the establishment of national independent authorities with powers and resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate remedies;

(j) To further develop or maintain, in this regard, preventive measures and remedies for violations and abuses of the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, as well as children;

(k) To consider developing, reviewing, implementing and strengthening gender-responsive policies that promote and protect the right of all individuals to privacy in the digital age;

(l) To provide effective and up-to-date guidance to business enterprises on how to respect human rights by advising on appropriate methods, including human rights due diligence, and on how to consider effectively issues of gender, vulnerability and/or marginalization;

(m) To promote quality education and lifelong educational opportunities for all to foster, inter alia, digital literacy and technical skills to effectively protect their privacy;

(n) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way;

(o) To protect individuals from violations or abuses of the right to privacy, including those which are caused by arbitrary or unlawful data collection, processing, storage and sharing, profiling and the use of automated processes and machine learning;

(p) To take steps to enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;

(q) To consider developing or to maintain legislation, preventive measures and remedies addressing harm from the processing, use, sale or multiple resale or other corporate sharing of personal data without the individual's free, explicit, meaningful and informed consent;

(r) To ensure that digital or biometric identity programmes are designed, implemented and operated after appropriate technical, regulatory, legal and ethical safeguards are in place and in full compliance with the obligations of States under international human rights law;

8. *Calls upon* all business enterprises, in particular those that collect, store, use, share and process data:

(a) To meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,²² including the right to privacy in the digital age, and to enhance efforts in this regard;

(b) To inform users in a clear, easily accessible and age-appropriate way about the collection, use, sharing and retention of their data that may affect their right to privacy, to refrain from doing so without their consent or a legal basis and to establish and to apply transparency policies that allow for the free, informed and meaningful consent of users, as appropriate;

(c) To implement administrative, technical and physical safeguards to ensure that data are processed lawfully and to ensure that such processing is limited to what is necessary in relation to the purposes of the processing and that the legitimacy of such purposes, as well as the accuracy, integrity and confidentiality of the processing, is ensured;

(d) To ensure that respect for the right to privacy and other international human rights is incorporated into the design, operation, evaluation and regulation of automated decision-making and machine-learning technologies and to provide for compensation for the human rights abuses that they may cause or to which they may contribute;

(e) To ensure that individuals have access to their personal data and to adopt appropriate measures for the possibility to amend, correct, update, delete and withdraw consent for the data, in particular if the data are incorrect or inaccurate, or if the data were obtained illegally;

(f) To put in place adequate safeguards that seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services, including where necessary through contractual clauses or notification of any relevant entities of abuses or violations when misuse of their products and services is detected;

(g) To enhance efforts to combat discrimination resulting from the use of artificial intelligence systems, including by exercising due diligence in assessing, preventing and mitigating the adverse human rights impacts of their deployment;

9. *Encourages* business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with the obligations of States under international

²² A/HRC/17/31, annex.

human rights law, and to enact policies that recognize and protect the privacy of individuals' digital communications;

10. *Encourages* States and, where applicable, business enterprises to systematically conduct human rights due diligence throughout the life cycle of the artificial intelligence systems that they conceptualize, design, develop, deploy, sell, obtain or operate, including regular and comprehensive human rights impact assessments and the participation of all relevant stakeholders;

11. *Encourages* all relevant stakeholders to mainstream a gender perspective into the conceptualization, development and implementation of digital technologies and related policies and promote the participation of women in order to address violence and discrimination against women and girls in digital contexts, inter alia, by encouraging digital technology companies, including Internet service providers, to respect standards and implement transparent and accessible reporting mechanisms;

12. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists and media workers to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use by journalists and media workers of such technologies and to ensure that any restrictions thereon comply with the obligations of States under international human rights law;

13. *Encourages* all relevant stakeholders to participate in informal dialogues about the right to privacy, and takes note with appreciation of the contribution of the Special Rapporteur of the Human Rights Council on the right to privacy to this process;

14. *Decides* to continue its consideration of the question at its seventy-ninth session.

*54th plenary meeting
15 December 2022*