United Nations A/HRC/RES/48/4

General Assembly

Distr.: General
13 October 2021

Original: English

Human Rights Council
Forty-eighth session
13 September–11 October 2021
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Resolution adopted by the Human Rights Council on 7 October 2021

48/4. Right to privacy in the digital age

The Human Rights Council,

Guided by the purposes and principles of the Charter of the United Nations,

Reaffirming the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights and other relevant international human rights instruments,

Recalling all previous General Assembly and the Human Rights Council resolutions on the right to privacy in the digital age, and the recent extension of the mandate of the Special Rapporteur on the right to privacy,[1] as well as other relevant resolutions,

Welcoming the work of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age,[2] noting with interest its reports thereon, and recalling the expert workshop on the right to privacy in the digital age, held by the Office of the High Commissioner on 27 and 28 May 2020, that noted the steadily growing impact of the use of artificial intelligence technologies on the exercise of the right to privacy, pointed to transparency concerns regarding personal data collection and exchanges underlying parts of artificial intelligence systems and expressed concern about adverse privacy impacts of the application of artificial intelligence,

Welcoming also the work of various special procedure mandate holders of the Human Rights Council on the right to privacy, and taking note of their contributions to the promotion and protection of the right to privacy,

Taking note of the Secretary-General's Road Map for Digital Cooperation, launched in June 2020,

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 other human rights,

[1] Resolution 46/16.
[2] See A/HRC/48/31.

including 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 that the right to privacy can enable the enjoyment of other rights, the free development of an individual's personality and identity and an individual's ability to participate in political, economic, social and cultural life,

Affirms that the same rights that people have offline must also be protected online, including the right to privacy, and noting that the accelerated synchronization of online and offline spaces can affect individuals, including their right to privacy,

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

Recognizing the need to further discuss and analyse, on the basis of 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 and the impact of surveillance on the enjoyment of 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 and to consider potential discriminatory effects,

Noting that the rapid pace of technological development enables individuals all over the world to use information and communications technology, 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, 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, persons with disabilities and older persons, as well as persons in vulnerable situations and marginalized groups,

Noting further that women and girls experience gender-specific violations and abuses of their right to privacy, both online and offline, as well as violations or abuses that have gender-specific impacts,

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

Acknowledging that human rights must be considered in the conception, design, use, deployment and further development of new and emerging technologies, such as those that involve artificial intelligence, as they can, without appropriate safeguards impact the enjoyment of the right to privacy and other human rights, and that the risks to these rights can and should be avoided or minimized, including by taking measures to ensure a safe, transparent, accountable, secure and high-quality data infrastructure, by exercising due diligence to assess, prevent and mitigate adverse human rights impacts, and by providing effective remedies, including judicial remedies, and redress mechanisms and establishing human oversight,

Recognizing that, despite its positive effects, the use of artificial intelligence that requires the processing of large amounts of data, often relating to personal data, including on an individual's behaviour, social relationships, private preferences and identity, can pose serious risks to the right to privacy, in particular when employed for identification, tracking, profiling, facial recognition, behavioural prediction or the scoring of individuals,

Emphasizing that privacy concerns should not be dismissed as a barrier to innovation,

Noting 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 also the public concern with regard to the intrusiveness and impact of data-gathering practices, the related impacts and harms stemming from surveillance and the increasing use of algorithms involved in the application of artificial intelligence systems,

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

Recognizing that racially and otherwise discriminatory outcomes must be prevented in the conception, design, development, deployment and use of new and emerging digital technologies,

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

Acknowledging 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, including their movements, social relationships, political activities, private preferences and identity,

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

Expressing concern that individuals 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 re-use, sale or multiple re-sale of their personal data, as the collecting, processing, use, storage and sharing of personal data, including sensitive data, has increased significantly in the digital age,

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 steps necessary to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant, *Emphasizing* that unlawful or arbitrary surveillance and/or interception of communications, the unlawful or arbitrary collection of personal data or unlawful or arbitrary hacking and the unlawful or arbitrary use of biometric technologies, as highly intrusive acts, violate or abuse the right to privacy, can interfere with other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association, and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale,

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 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,

Recalling that business enterprises have a responsibility to respect human rights, as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, and that the obligation and the primary responsibility to promote and protect human rights and fundamental freedoms lie with the

State, and welcoming the work of Office of the United Nations High Commissioner for Human Rights on the application of these principles on digital technologies,

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for 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,

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 fighting the COVID-19 pandemic, and recalling in this regard the importance of protecting health-related 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. *Recalls* that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality;

3. *Also recalls* the increasing impact of new and emerging technologies, such as those developed in the fields of surveillance, artificial intelligence, automated decision-making and machine-learning and of profiling, tracking and biometrics, including facial and emotional recognition, without proper safeguards, on the enjoyment of the right to privacy and other human rights, including the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association;

4. *Affirms* that the same rights that people have offline must also be protected online, including the right to privacy;

5. *Acknowledges* that risks to the right to privacy and other human rights can and should be minimized by adopting adequate regulation or other appropriate mechanisms, in accordance with applicable obligations under international human rights law in the conception, design, development and deployment of new and emerging digital technologies, such as artificial intelligence, by ensuring a safe, secure and high-quality data infrastructure, by exercising due diligence to assess, prevent and mitigate adverse human rights impacts, and by establishing human oversight, as well as redress mechanisms;

6. *Calls upon* all States:

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

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

(c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, 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;

(d) To ensure that any measures taken to counter terrorism and violent extremism conducive to terrorism that interfere with the right to privacy are consistent with the

principles of legality, necessity and proportionality and comply with their obligations under international law;

(e) To ensure that biometric identification and recognition technologies, including facial recognition technologies by public and private actors do not enable arbitrary or unlawful surveillance, including of those exercising their right to freedom of peaceful assembly;

(f) To develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely, through the unlawful or arbitrary collection, processing, retention or use of personal data by individuals, Governments, business enterprises or private organizations;

(g) To consider adopting or reviewing legislation, regulations or policies to ensure that business enterprises fully incorporate the right to privacy and other relevant human rights into 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 reparation and guarantees of non-repetition;

(h) To further develop or maintain in this regard preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, children, persons in vulnerable situations or marginalized groups;

(i) To develop, review, implement and strengthen gender-responsive policies that promote and protect the right of all individuals to privacy in the digital age;

(j) 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;

(k) To refrain from the use of surveillance technologies in a manner that is not compliant with international human rights obligations, including when used against journalists and human rights defenders, and to take specific actions to protect against violations of the right to privacy, including by regulating the sale, transfer, use and export of surveillance technologies;

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

(m) To ensure the availability of relevant training for judges, lawyers, prosecutors and other relevant practitioners in the justice system on the functioning of new and emerging digital technologies and their impact on human rights;

(n) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way, and to protect individuals from harm, including that caused by business enterprises through data collection, processing, storage and sharing and profiling, and the use of automated processes and machine learning;

(o) To consider appropriate measures that would enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;

(p) To develop or maintain legislation, preventive measures and remedies that address damage caused by the processing, use, sale or multiple resale or other corporate sharing of personal data without the individual's free, explicit and informed consent;

(q) To take appropriate measures to ensure that digital or biometric identity programmes are designed, implemented and operated with appropriate legal and technical safeguards in place and in full compliance with international human rights law;

(r) To enhance efforts to combat discrimination resulting from the use of artificial intelligence systems including by exercising due diligence to assess, prevent and mitigate their adverse human rights impacts of their deployment;

7. *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 international human rights instruments;

8. *Encourages* all business enterprises, in particular business enterprises 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, including the right to privacy in the digital age, and to enhance efforts in this regard;

(b) To inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and refrain from doing so without their consent or a legal basis, and to establish transparency and policies that allow for the informed consent of users;

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

(d) To ensure that individuals have access to their data and the possibility to amend, correct, update and delete the data, in particular if the data are incorrect or inaccurate or if the data were obtained illegally;

(e) To ensure that the respect for the right to privacy and other relevant human rights is incorporated into the design, operation, evaluation and regulation of automated decision-making and machine-learning technologies, and to provide effective remedies, including compensation, for human rights abuses that they have caused or to which they have contributed;

(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, and promptly inform relevant domestic, regional or international oversight bodies 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 through human rights due diligence and monitoring and evaluation of artificial intelligence systems across their life cycle, and the human rights impact of their deployment;

9. *Encourages* business enterprises, including communications service providers, to work towards enabling solutions to secure and protect the confidentiality of digital communications and transactions, including measures for encryption, pseydonymization and anonymity, and to ensure the implementation of human-rights compliant safeguards, and calls upon States not to interfere with the use of such technical solutions with any restrictions thereon complying with States' obligations under international human rights law, and to enact policies that protect the privacy of individuals' digital communications;

10. *Encourages* States and, where applicable, business enterprises to conduct human rights due diligence throughout the life cycle of the artificial intelligence systems they design, develop, deploy or sell or obtain and operate;

11. *Requests* the Office of the United Nations High Commissioner for Human Rights to prepare a written report identifying recent trends and challenges with regard to the human right to privacy, including those addressed in the present resolution, to identify and clarify related human rights principles, safeguards and best practices, and to present the report to the Human Rights Council at its fifty-first session, to be followed by an interactive dialogue;

12. *Requests* the Office of the High Commissioner, when preparing the above-mentioned report, to seek input from and to take into account the work already done by

relevant stakeholders from diverse geographical regions, including States, international and regional organizations, the special procedures of the Human Rights Council, the treaty bodies, other relevant United Nations offices, agencies, funds and programmes, within their respective mandates, national human rights institutions, civil society, the private sector, the technical community and academic institutions.

41st meeting
7 October 2021

[Adopted without a vote.]