United Nations A/HRC/RES/54/21

General Assembly

Distr.: General
16 October 2023

Original: English

Human Rights Council
Fifty-fourth session
11 September–13 October 2023
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 12 October 2023

54/21. 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 Human Rights Council resolutions on the right to privacy in the digital age, 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, and welcoming also the work of various special procedure mandate holders of the Human Rights Council on the right to privacy and their contributions to the promotion and protection of the right to privacy,

Reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with their 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, 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 is intrinsically linked to the effective protection of every individual's personal data,

Recognizing also 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,

Reaffirming 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, and that the processing of personal data must be subject to human rights safeguards and restrictions, especially the data of persons in vulnerable situations,

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, and recognizing that the way in which many digital platforms are designed, commercialized, maintained and governed can give rise to disinformation, misinformation and hate speech, which can exacerbate gender stereotypes, result in sexual and gender-based violence and undermine the data protection and the fulfilment of all women's and girls' rights, in particular their right to privacy,

Noting that children can be particularly vulnerable to abuses and violations of their right to privacy, including through cyberbullying, cyberstalking and sexual abuse and exploitation, and noting also that States parties must implement the Convention on the Rights of the Child 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,

Acknowledging the need to exercise human rights due diligence in the conception, design, use, acquisition, transfer, sale, 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 and periodic reviews of already deployed technologies 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 digital technologies and artificial intelligence systems that require the processing of large amounts of data, often relating to personal data, including on an individual's behaviour, social relationships, private preferences and identity, including metadata, 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,

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, and can result in intensifying threats from misinformation, disinformation and hate speech, in particular on social media platforms, which may lead to violence, including political violence, and recalling in this regard the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,

Noting with concern 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 also that certain predictive algorithms and the increasing use of facial recognition and surveillance technologies are likely to result in discrimination, in particular when data used in the training of algorithms are not accurate, relevant and representative and audited against encoded bias,

Noting that the use of artificial intelligence may, without human rights safeguards, pose the risk of reinforcing discrimination, including structural inequalities, especially when processing sensitive data, and recognizing that racially and otherwise discriminatory outcomes must be prevented in the design, development, implementation and use of new and emerging digital technologies,

Noting with concern reports indicating lower accuracy of biometric data identification, including facial recognition technologies that show racial identification biases and prejudices against women, including when non-representative training data are used, and that the use of digital technologies can reproduce, reinforce and even exacerbate racial and gender inequalities, and recognizing 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, and as such recalling that service providers should take steps to minimize, obscure or delete metadata and to reduce the traceability of users' metadata in order to strengthen the protections afforded by encryption and protect the right to privacy,

Recognizing that a lack of access to affordable and reliable technologies and services remains a critical challenge in many developing countries, especially to bridging the digital divides, including both between and within countries and the gender digital divide, and to accelerating progress towards development in its various forms, including achieving the Sustainable Development Goals, and stressing in this regard that many States, including developing countries, all over the world need support to bridge these digital divides and to meet the Sustainable Development Goals,

Recognizing also the need to ensure that international human rights law is respected, including by conducting human rights impact assessments in the conception, design, development, deployment, evaluation, regulation and technical standard-setting of data-driven technologies, and to ensure that they are subject to adequate safeguards and oversight,

Expressing concern that individuals, in particular 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 collecting, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age, and that if personal and sensitive data are disclosed, exceptional damage, injury or hardship may be caused to individuals,

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 be consistent with the principles of legality, necessity and proportionality, 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,

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, including through the use of malware or spyware, 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, including technology companies, 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 the Office of the High Commissioner 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, and recognizing that States must promote such measures and refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking and restrictions on accessing and using encryption technology,

Stressing 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 and legitimacy with regard to the aim pursued, necessity and proportionality and the need to protect human rights, including the right to privacy, as well as to protect personal data in the response to health or other emergencies, and stressing also the need to delete or anonymize the data gathered once they ceased to fulfil the purposes for which they were collected,

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 recognition, without human rights safeguards, present to the full enjoyment of the right to privacy and other human rights, and acknowledges that some applications may not be compatible with international human rights law;

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

5. *Also affirms* that, in order to protect, respect and promote the right to privacy, personal data should only be collected for specified, explicit and legitimate purposes and must be processed lawfully, fairly and in a transparent manner;

6. *Highlights* that every person should be able to ascertain which public authorities or private individuals or bodies control or may control their personal data, and that any interference with data protection must be lawful, in accordance with international human rights law, including the principles of legality, proportionality, necessity and non-discrimination;

7. *Acknowledges* that risks to the right to privacy and other human rights can and should be minimized by adopting adequate regulations or other appropriate mechanisms, in

accordance with applicable obligations under international human rights law, in the conception, design, use, acquisition, transfer, sale, deployment and further development 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;

8. *Stresses* that States must comply with their human rights obligations and that business enterprises, including technology companies, should respect the right to privacy and other human rights when collecting, processing, sharing and storing personal data by, inter alia, adopting data protection policies and safeguards;

9. *Also stresses* that remote biometric surveillance systems, including facial recognition, raise serious concerns with regard to their proportionality, given their highly intrusive nature and broad impact on large numbers of people;

10. *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, especially in the case of persons in vulnerable situations or marginalized groups;

(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 respect international human rights obligations, including the right to privacy, when States 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;

(e) 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;

(f) 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;

(g) 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;

(h) 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 collection, processing, retention or use of personal data by individuals, Governments, business enterprises or private organizations without the individual's free, explicit and informed consent or unless otherwise lawful, in accordance with international human rights law;

(i) To consider adopting or maintaining data protection legislation, regulations and policies, including on digital communication data, that comply with their international human rights obligations and that could include provisions on sensitive personal data protection and the establishment of national independent authorities with the powers and

resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate effective remedies;

(j) To consider adopting or reviewing legislation, regulations or policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully incorporate the right to privacy and other relevant human rights into the design, development, deployment and evaluation of technologies, including artificial intelligence, to take appropriate steps to improve and encourage corporate accountability, 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;

(k) 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;

(l) To develop, review, implement and strengthen gender-responsive policies and programmes that contribute to the empowerment of all women and girls and promote and protect the right of all individuals to privacy in the digital age;

(m) 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, and 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;

(n) To refrain from the use of surveillance technologies in a manner that is not compliant with international human rights obligations, including when used against human rights defenders, journalists and other media workers, 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;

(o) To promote accessible, inclusive quality education and lifelong education opportunities for all to foster, inter alia, digital and data literacy and the technical skills, including by providing online safety training, guidance and awareness-raising, required to protect effectively their privacy, and to ensure the availability of appropriate training for relevant stakeholders in this area;

(p) 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;

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

11. *Encourages* all business enterprises, in particular business enterprises that collect, store, use, share and process data:

(a) To review their business models and ensure that their design and development processes, business operations, data collection and data processing practices are in line with the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, and to emphasize the importance of conducting human rights due diligence of their products, in particular of the role of algorithms and ranking systems;

(b) To inform users, in a clear and age-appropriate way that is easily accessible, including for persons with disabilities, 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 transparency and policies that allow for the free, informed and meaningful consent of users;

(c) To integrate the right to privacy and other relevant human rights into internal policymaking, product engineering, business development, staff training and other relevant internal processes;

(d) To implement administrative, technical and physical safeguards to ensure that data are processed lawfully, 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, and to prevent the unauthorized disclosure or use of data;

(e) To ensure that individuals have access to their data and the possibility to amend, correct, update, delete and withdraw consent for the use of their data, in particular if the data are incorrect or inaccurate or if the data were obtained illegally or used for discriminatory purposes;

(f) To ensure that 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 or been linked;

(g) 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 to promptly inform relevant domestic, regional or international oversight bodies of abuses or violations when misuse of their products and services is detected;

(h) 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;

(i) To promote the transparency and adequate explainability of algorithmic decision-making, automated systems and human-in-the-loop systems, and to ensure that data used for the training of algorithms are representative and legally collected;

(j) To put in place appropriate safeguard measures to ensure that the distribution and transfer of data within and among organizations and/or the rearrangement of data, including through cloud computing, unstructured datasets, blockchain technology, augmented reality and the Internet of things, are compatible with data protection and the right to privacy;

(k) To take appropriate measures throughout the life cycle of artificial intelligence systems and digital technologies, including before commencing the design and development of applications and software that involve processing personal data, with a view to establishing a risk monitoring and management system to ensure that data are processed fairly and lawfully;

12. *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, pseudonymization and anonymity, and to ensure the implementation of human-rights compliant safeguards, and calls upon States to promote measures and technical solutions for strong encryption, pseudonymization and anonymity, 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;

13. *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 or sell or obtain and operate, including through regular and comprehensive human rights impact assessments and the participation of all relevant stakeholders;

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

15. *Requests* the Office of the United Nations High Commissioner for Human Rights to prepare a report on challenges and risks with regard to discrimination and unequal enjoyment of the right to privacy associated with the collection and processing of data, 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-seventh session, to be followed by an interactive dialogue;

16. *Also 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.

48th meeting
12 October 2023

[Adopted without a vote.]