United Nations A/HRC/RES/42/15

General Assembly

Distr.: General
7 October 2019

Original: English

Human Rights Council
Forty-second session
9–27 September 2019
Agenda item 3

Resolution adopted by the Human Rights Council on 26 September 2019

42/15. The 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, the Convention on the Rights of the Child and the Convention on the Rights of Persons with Disabilities, and other relevant international human rights instrument,

Reaffirming also the Vienna Declaration and Programme of Action,

Reiterating the universality, indivisibility, interdependence and interrelatedness of all human rights and fundamental freedoms,

Recalling all previous General Assembly and the Human Rights Council resolutions on the right to privacy in the digital age, as well as other relevant resolutions,

Recalling also 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,

Welcoming the work of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age,[1] noting with interest its reports thereon, and recalling the expert workshop on the right to privacy in the digital age held by the Office on 19 and 20 February 2018,

Welcoming also the work of the Special Rapporteur on the right to privacy, and taking note of his reports, as well as of the contributions to the promotion and protection of the right to privacy made by other special procedures of the Human Rights Council,

Taking note of the Secretary-General's strategy on new technologies, including the work of the High-level Panel on Digital Cooperation and its report *The Age of Digital Interdependence* submitted to the Secretary-General on 10 June 2019,

[1] A/HRC/39/29.

Noting the adoption of the principles on personal data protection and privacy by the High-level Committee on Management on 11 October 2018,

Noting with appreciation general comment No. 16 (1988) of the Human Rights Committee on the right to privacy, and its recommendation that States take effective measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises, while also noting the vast technological leaps that have taken place since its adoption and the need to address the right to privacy in view of the challenges of the digital age,

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, 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 and the free development of an individual's personality and identity, and 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 privacy might affect the enjoyment 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,

Recalling that the General, Assembly in its resolution 73/179 of 17 December 2018, encouraged the Human Rights Council to remain actively seized of the debate, and invited all relevant stakeholders to further discuss how profiling, automated decision-making and machine-learning technologies, sometimes referred to as artificial intelligence, without proper safeguards, impact the enjoyment of the right to privacy, for the purpose of clarifying existing principles and standards and identifying best practices regarding the promotion and protection of the right to privacy,

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

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, 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 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 may affect all individuals, with particular effects on women, as well as children, persons with disabilities and those who are vulnerable and marginalized,

Recognizing the need for Governments, the private sector, international organizations, civil society, the technical and academic communities and all relevant stakeholders to be cognizant of the impact, opportunities and challenges of rapid technological change on the promotion and protection of human rights, as well as of its potential to facilitate efforts, to accelerate human progress and to promote and protect human rights and fundamental freedoms,

Noting that the use of artificial intelligence can contribute to the promotion and protection of human rights, and can also have far-reaching and global implications, including

with regard to the right to privacy, that are transforming Governments and societies, economic sectors and the world of work,

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,

Noting that the use of artificial intelligence may, without adequate safeguards, pose the risk of reinforcing discrimination, including structural inequalities,

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, social relationships, private preferences and identity,

Noting with concern that automatic processing of personal data for individual profiling, automated decision-making and machine learning technologies may, without adequate safeguards, lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to apply international human rights law in the design, development, deployment, evaluation and regulation of these 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,

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,

Emphasizing also 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, 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 respect 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 of data protection policies and safeguards,

Noting also that, while the prevention and suppression of terrorism and violent extremism conducive to terrorism is a public interest of great importance, and 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,

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, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques,

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

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

5. *Acknowledges* that the use, deployment and further development of new and emerging technologies, such as artificial intelligence, can impact the enjoyment of the right to privacy and other human rights, and that the risks to the right to privacy can and should be minimized by adopting adequate regulation or other appropriate mechanisms, including by taking into account international human rights law in the design, development and deployment of new and emerging technologies, such as artificial intelligence, by ensuring a safe, secure and high-quality data infrastructure and by developing human-centred auditing mechanisms, 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;

(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 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 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 and 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, and children and persons in vulnerable situations or marginalized groups;

(i) 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;

(j) 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;

(k) 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;

(l) 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;

(m) 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;

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;

(b) To inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency and policies that allow for the informed 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 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 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;

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 and anonymity, 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;

10. *Requests* the United Nations High Commissioner for Human Rights to organize, before the forty-fourth session of the Human Rights Council, a one-day expert seminar to discuss how artificial intelligence, including profiling, automated decision-making and machine-learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy, to prepare a thematic report on the issue and to submit it to the Council at its forty-fifth session;

11. *Encourages* States, relevant United Nations agencies, funds and programmes, intergovernmental organizations, treaty bodies, the special procedures, regional human rights mechanisms, civil society organizations, academia, national human rights institutions, business enterprises, the technical community and other relevant stakeholders to participate actively in the expert seminar;

12. *Decides* to continue its consideration of the matter under the same agenda item.

39th meeting
26 September 2019

[Adopted without a vote.]