United Nations A/HRC/40/63

General Assembly

Distr.: General
16 October 2019

Original: English

Human Rights Council
Fortieth session
25 February–22 March 2019
Agenda item 3
Promotion and protection of all human rights, civil political, economic, social and cultural rights, including the right to development

Right to privacy

Report of the Special Rapporteur on the right to privacy*

Summary

In his report, prepared pursuant to Human Rights Council resolutions 28/16 and 37/2, the Special Rapporteur on the right to privacy focuses on intelligence oversight issues and provides links to the first report on the work on privacy and gender of the Task Force on Privacy and Personality and that of the Task Force on Health Data.

* The present report was submitted after the deadline so as to include the most recent information.

GE.19-17878(E)

1917878

Contents

I. Overview of activities

1. Since March 2018, the Special Rapporteur on the right to privacy has advanced the mandate by examining relevant information, including challenges arising from new technologies; undertaking official and "non-official" country visits; promoting the protection of the right to privacy; advocating privacy principles; contributing to international events to promote a coherent approach to the right to privacy; raising awareness of the right to privacy and effective remedies; and reporting on alleged violations.

2. The Special Rapporteur submitted a report to the General Assembly in October 2018 on big data and open data (A/73/438).

3. The Special Rapporteur's activities since his 2018 annual report to the Human Rights Council (A/HRC/37/62) have included:

(a) Advancing, with task force chairs, the work of five thematic action stream task forces on big data and open data; health data; privacy and personality; security and surveillance; and the use of personal data by corporations;

(b) A total of 24 communications to Member States raising matters concerning the right to privacy, and 14 press releases and statements;[1]

(c) Official country visits to the United Kingdom of Great Britain and Northern Ireland (June 2018) and Germany (November 2018);

(d) International keynote and other papers;[2]

(e) Consulting a range of bodies, for example, the Irish Council for Civil Liberties; the Japan Civil Liberties Union; the Japan Federation of Bar Associations; Privacy International; and the Northern Ireland Human Rights Commission; and engaging in multiple activities at the Internet Governance Forum, and RightsCon, among many others;

(f) Exchanging information with: Governments (at the national and subnational levels); data protection and privacy commissioners; Chairperson, European Union Article 29 Data Protection Working Party; Chairperson, Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); standards setting organizations, such as: the International Telecommunication Union; the Institute of Electrical and Electronics Engineers; civil society organizations; permanent missions to the United Nations Office at Geneva; special procedures mandate holders, the Office of the United Nations High Commissioner for Human Rights; researchers; academics; and professional bodies.

II. Privacy in context

4. The right to privacy can facilitate the enjoyment of other human rights. Equally, infringements thereof constrain the enjoyment of other human rights.

5. There are several historical examples of Member States ratifying international instruments on human rights while lacking the genuine will to take the necessary measures for their implementation. One such was the German Democratic Republic, which, by ratifying the International Covenant on Civil and Political Rights on 8 November 1973, took upon itself the obligation to respect, inter alia, the right to privacy (art. 17), while maintaining a surveillance regime known for its widespread and systematic violations of the privacy of a large number of its citizens.

6. Regrettably, the Special Rapporteur often finds similar contradictions today: while most Member States unequivocally commit themselves to protecting the right to privacy,

[1] A total of 18 letters and 6 press releases were jointly issued with other Special Rapporteurs.

[2] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex1_Keynotes.pdf.

many are acting in ways that increasingly put it at risk, by employing new technologies that are incompatible with the right to privacy, such as big data and health data, infringing the dignity of its citizens on the basis of gender or gender identity and expression, and arbitrarily surveying their own citizens.

7. The right to self-determination, as proclaimed in article 1 (1) of the International Covenant on Civil and Political Rights, allows all peoples to determine their political status and freely pursue their development. Similarly, all basic liberties in the Covenant, including the right to freedom of movement (art. 12) or the right to freedom of association (art. 22), the right to freedom of religion (art. 18), the right to freedom of expression (art. 19) and the right to privacy (art. 17), protect the right of all individuals to their personal autonomy. The right of a citizen to choose what, when, where and how to be, whom to be with and what to think and say are part of the inalienable rights that countries have agreed to protect under the Covenant.

8. The right to privacy is integral to discussions about personal autonomy. As early as 1976, Paul Sieghart identified the following links between privacy, information flows, autonomy and power:

> In a society where modern information technology is developing fast, many others may be able to find out how we act. And that, in turn, may reduce our freedom to act as we please – because once others discover how we act, they may think that it is in their interest, or in the interest of society, or even in our own interest to dissuade us, discourage us, or even stopping us from doing what we want to do, and seek to manipulate us to do what they want to do.[3]

9. The Special Rapporteur linked that position to privacy in the following way:

> Shorn of the cloak of privacy that protects him, an individual becomes transparent and therefore manipulable. A manipulable individual is at the mercy of those who control the information held about him, and his freedom, which is often relative at best, shrinks in direct proportion to the extent of the nature of the options and alternatives which are left open to him by those who control the information.[4]

10. That is why privacy is so closely linked to meaningful personal autonomy. Infringement of privacy is often part of a system which threatens other liberties. It is often carried out by State actors to secure and retain power, but also by non-State actors, such as individuals or corporations wishing to continue to control others. That is why, in many cases, the Special Rapporteur must consider how violations of the right to privacy are linked to other violations.

Privacy as a qualified right and the standard of necessity in a democratic society

11. The right to privacy is not an absolute right but a qualified right. It may be limited, but always in a very carefully delimited way. According to the standard established in article 17 of the International Covenant on Civil and Political Rights, interferences with the right to privacy are permissible under international human rights law only if they are neither arbitrary nor unlawful. The Human Rights Committee explained in its general comment No. 16 (1988) on the right to privacy that the term "unlawful" means that any interference be envisaged by the law and that the law itself must comply with the provisions, aims and objectives of the Covenant. The concept of arbitrariness, according to the Committee, guarantees that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

12. In its general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant, the Human Rights Committee stipulates that States parties must refrain from violation of the rights recognized by the Covenant, and that

[3] Paul Sieghart, *Privacy and Computers* (London, Latimer New Dimensions, 1976), p. 24.

[4] Joseph A. Cannataci, *Privacy and Data Protection Law: International Development and Maltese Perspectives* (Oslo, Norwegian University Press, 1986), p. 60.

any restrictions on any of those rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. The Committee further underscores that in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.

13. The term "necessary in a democratic society" is explicitly cited in two articles of the International Covenant on Civil and Political Rights: article 21 (right of peaceful assembly) and article 22 (freedom of association), but not in article 17.

14. Article 8 (2) of the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) is explicit as to the nature of the qualification:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

15. Democracy was proclaimed as part of the essential context for the enjoyment of human rights in the 1948 Universal Declaration of Human Rights, wherein the concept of "the general welfare in a democratic society" appeared in article 29. The interplay between the authors and signatories of the European Convention on Human Rights, adopted in 1950, and the authors of the International Covenant on Civil and Political Rights continued for the best part of 15 years, until the launch of the latter in 1966. The concept of "necessary in a democratic society" is present in at least six articles of the European Convention, including article 8, cited above, then transposed into the Covenant and best exemplified by article 22 (1):

> No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others.

16. Article 22, however, relates to freedom of assembly and not to the right to privacy. It is for historians examining the development of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights to explain why the wording "necessary in a democratic society" is explicit in articles 21 and 22 and not in article 17, but the Special Rapporteur must reasonably apply the same standard, that is to say that the right can be qualified only by measures provided for by law (art. 17 (2)) and that such measures must be necessary in a democratic society by way of an interpretation of "arbitrary or unlawful interference", consistent with articles 14, 21 and 22 of the Covenant.

17. This interpretation is consistent with paragraph 2 of resolution 34/7 of the Human Rights Council, in which it reaffirms that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality, reflecting the terms used in the jurisprudence of the Human Rights Committee (CCPR/C/USA/CO/4, para. 22).

18. The essential, four-fold test is then that any legitimate infringement of privacy cannot be: (a) arbitrary and must be provided for by law; (b) for any purpose but for one which is necessary in a democratic society; (c) for any purpose except for those of "national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others"; and, (d) the measure must be proportionate to the threat or risk being managed.

19. The dual tests of "necessity" and "necessity in a democratic society" are essential ones for any measure taken by a Member State which may be held to infringe privacy. They must also be taken into account when examining infringements of other rights whose exercise depends on the right to privacy.

20. The context for privacy and the links between autonomy, privacy and necessary measures in a democratic State explain why the Special Rapporteur is prioritizing States with solid democratic institutions and safeguards, as those are the contexts where his intervention is more likely to have a positive impact on the enjoyment of the right to privacy. In countries where democratic safeguards are weaker, he is seeking to identify opportunities to intervene positively.

21. During 2019 and 2020, the Special Rapporteur will be focusing further on Africa, Asia and South America, with one visit scheduled in each of those regions; but he will continue to monitor the situation in other countries with the assistance of civil society, inter alia. This is not insensitivity to the experiences of privacy in other regions of the world. It is not possible to investigate those experiences in the detail or manner that the Special Rapporteur would wish, on account of three factors: time, resources and opportunity to carry out meaningful investigations on the ground. Thus, the Special Rapporteur will continue to monitor those States where the rule of law is replaced by the "rule by law" and where the law becomes an instrument of regime control and oppression. He will assess the creation of cybercrime legislation in the Middle East and North Africa region, which may be posing a risk to the enjoyment of the right to privacy.[5]

Privacy, technology and other human rights from a gender perspective

22. The present report presents the first results of the Special Rapporteur's ongoing work on privacy and gender. The Task Force on Privacy and Personality will continue its work on the link between privacy and equality of genders regardless of form or expression. In addition to consultation on the report,[6] the Special Rapporteur plans to devote more attention over the next three years to this area, including the links between privacy, autonomy and the male guardianship system present to varying degrees in a number of countries.

23. Member States wishing to participate in consultations on privacy and gender should register their interest by 31 March 2019.

Privacy and health data

24. The present report also provides details of the Special Rapporteur's continuing work on privacy and health data. Like the gender work, there are major emerging issues, such as genetics, genome research and biobanking. A question before the Special Rapporteur is that of whether it is necessary and proportionate for the entire population of a given country to have its DNA data collected. The Special Rapporteur's mandate will be engaging on these matters with States legislating such measures.

25. The Task Force on Health Data has identified issues ranging from matters concerning indigenous data sovereignty, prisoner populations, forensic databases, "smart" implanted health devices, devices/prostheses that transmit ongoing real-life data back to companies, inter alia, thereby positioning the "body as data" and subject to use in legal proceedings, and artificial intelligence/machine learning and automatic processing. These matters will be explored in consultations during 2019.

III. Security and surveillance

26. The Special Rapporteur's mandate arose from the international furore surrounding the revelations by Edward Snowden about the activities of intelligence agencies, in particular concerning national security protection.

27. To reinforce privacy safeguards in the intelligence field, the Special Rapporteur initiated the International Intelligence Oversight Forum, which has held conferences in

[5] Wafa Ben-Hassine and Dima Samaro, "Restricting cybersecurity, violating human rights: cybercrime laws in MENA region", Open Global Rights, 10 January 2019.

[6] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf.

Bucharest in 2016, Brussels in 2017 and Valletta in 2018. Following the 2018 conference, the Special Rapporteur reports:

(a) Recent regional initiatives such as the European Union General Data Protection Regulation[7] (effective 25 May 2018) and Police Directive[8] (effective 6 May 2018), while important, are insufficient for extending privacy protection to the field of national security, including the oversight of intelligence activities undertaken for national security purposes.[9]

(b) The modernization of Convention 108,[10] a recent global initiative formally launched on 10 October 2018, in which 70 of the United Nations 193 Member States have participated, is commended for its article 11, with its high-level set of principles and safeguards which, unlike the General Data Protection Regulation, are also applicable to activities undertaken for national security purposes.

28. In his 2018 report to the General Assembly (A/73/438), the Special Rapporteur recommended that all Member States be encouraged to ratify the modernized Convention (Convention 108+). In the context of intelligence oversight and national security activities which may be privacy intrusive, the immediate deployment by United Nations Member States of the standards and safeguards outlined in article 11 of Convention 108+, is appropriate for the protection of the fundamental right to privacy.

29. These key safeguards and standards, in particular those of proportionality and necessity, informed the reasoning of two landmark judgments of the European Court of Human Rights in 2018, both of which are closely related to the activities of intelligence services: *Centrum för Rättvisa v. Sweden* (19 June 2018) and *Big Brother Watch and others v. the United Kingdom* (13 September 2018).

30. These judgments have a potential worldwide impact given the wide membership of the Council of Europe, with 47 member States, and the global reach of intelligence services from the region.

31. The Special Rapporteur supports the strict application of the tests of proportionality and necessity in a democratic society as an important benchmark with global repercussions. The intelligence agencies in other regions may be influenced by the increasingly strict standards applied in Europe. Intelligence analysis containing personal information and other personal data transferred from and to Europe thus needs to come under correspondingly strict oversight to ensure that these privacy-respectful standards are upheld in Europe and serve as a possible good practice and model worldwide.

32. It is important to note that the qualifier “a democratic society”, is a fundamental part of the test when evaluating the legal protections afforded in any United Nations Member State. A number of new technologies, in particular the Internet, smartphones, big data analytics, wearables, smart energy and smart cities, render individuals and communities more vulnerable to government surveillance of corporations in their countries, as well as by the intelligence agencies of foreign States and corporations.

33. The potential for States to use new technologies in this way is a significant risk to privacy and other human rights, such as freedom of expression, freedom of association and freedom of religion or belief. The discrete and cumulative effects of these technologies give the State the ability to closely profile and monitor the behaviour of individuals in new ways and to an unprecedented extent.

34. These technologies may be used to undermine human rights and democracy. Democracy may be an imperfect mechanism but, historically, it has provided the best

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

[9] The European Union lacks competence in the field of national security, and therefore cannot adequately extend privacy protection to activities in this field, including oversight of intelligence activities for the purpose of national security.

[10] Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data.

ecosystem possible for nurturing human rights. Impacts upon democracy are thus a key base metric against which privacy-intrusive measures must be evaluated.

35. The Special Rapporteur will continue to implement his global mandate in cooperation with all Member States, even if he is aware that the success of his cooperation and, ultimately, the respect for the right to privacy, is likelier in those countries that enjoy solid democratic institutions and safeguards.

36. Throughout 2018, a key concern was what happens to intelligence analysis containing personal data once shared by the intelligence service or law-enforcement agency of one country with those of another country. Are the data, and thus the privacy of the individuals concerned, protected by the same standards in the receiving State as those upheld in the transmitting State? The importance of this warrants action as recommended.

37. On 14 November 2018, five oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland, all parties to Convention 108, and therefore bound by its provisions imposing constraints on the use of personal data for national security purposes, issued a joint statement concerning a potential oversight gap and ways to tackle this risk when overseeing international data exchange by intelligence and security services.[11] This is an important and welcome development brought to the attention of the international community.

38. Participants at the International Intelligence Oversight Forum 2018 considered that initiative an important parallel development to the establishment of the Five Eyes Intelligence Oversight and Review Council of the agencies responsible for the oversight of intelligence within the Five Eyes alliance: Australia, Canada, New Zealand, the United Kingdom and the United States. The Special Rapporteur welcomes the establishment and activities of the Council, especially given the location and global reach of the five States which form the alliance. Since 2013, each of these States has introduced legislative reform to reinforce the oversight and privacy safeguards related to intelligence activities in the national security and other sectors. The reforms of some of these States have been more comprehensive than others; the latest legislation in Australia, for instance, has been identified by the mandate holder as a cause of concern from a privacy protection point of view.[12]

39. The United Kingdom Investigatory Powers Commissioner's Office issued a statement[13] welcoming the declaration by the oversight agencies of Belgium, Denmark, the Netherlands, Norway and Switzerland. The Office has the potential and perhaps even a special responsibility inherent to its geographical location, to provide a bridge between continental European oversight agencies and those collaborating on the Council.

40. The Special Rapporteur will facilitate and support this and other initiatives to the extent that they lead to the embedding of international human rights standards and safeguards relating to the exchange of personal information between the intelligence services and law enforcement agencies of one country with those of another.

41. The oversight of intelligence activities was the main focus of the Special Rapporteur's contribution during the proceedings of the European Data Protection Board in its consideration of the adequacy of the national law and safeguards of Japan. The Special Rapporteur's submissions and evidence were discussed at the debate, leading to the rejection[14] on 5 December 2018, for a period, of an adequacy finding regarding Japan.

42. In September 2018, the European Court of Human Rights found that the United Kingdom bulk interception regime violated article 8 of the European Convention on Human Rights (right to respect for private and family life/correspondence) owing to insufficient

[11] See https://english.ctivd.nl/documents/publications/2018/11/14/index.

[12] Submission by the Special Rapporteur to the Australian Joint Parliamentary Committee Intelligence and Security, No. 81. 2018, available at www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1/section?id=committees%2freportjnt%2f024247%2f26914.

[13] See www.ipco.org.uk/docs/IPCO%20Statement%20re%205%20oversight%20bodies.docx.

[14] See https://edpb.europa.eu/news/news_en.

oversight of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, and to inadequate safeguards for selection of "related communications data" for examination:[15]

(a) The Court held that the regime for obtaining communications data from communications service providers violated article 8; and that the regimes for bulk interception and for obtaining communications data from communications service providers violated article 10 of the Convention owing to insufficient safeguards for confidential journalistic material;

(b) It further found that the regime for sharing intelligence with foreign Governments did not violate either article 8 or article 10.

43. While this judgment concerned the previous United Kingdom statutory surveillance framework, its findings are very significant and are brought to the attention of Member States for review of their practices and frameworks.

44. This development highlights the importance of detailed and effective safeguards – legal and procedural – in national law and in the practices of intelligence agencies and their oversight authorities.

45. During the Special Rapporteur's official visit to Germany in November 2018, good practices in the exercise of bulk powers were debated, and a related compendium of such good practices developed by the Stiftung Neue Verantwortung[16] (November 2018) (is recommended for the consideration of States.

Recommendations

46. The Special Rapporteur recommends:

(a) The incorporation by Member States into their national legal systems of the standards and safeguards set out in Convention 108+, article 11, for the protection of the fundamental right to privacy, in particular:

(i) The creation of legal certainty by ensuring that any and all privacy-intrusive measures, even for the purposes of national security, defence and public safety, as well as the prevention, investigation and prosecution of crime are provided for by laws which are the subject of proper public consultation and parliamentary scrutiny;

(ii) The establishment of the test of "a necessary and proportionate measure in a democratic society" as the key metric which internal compliance units within intelligence and law enforcement agencies must apply to any privacy-intrusive measure and against which the actions of such agencies will be measured and held accountable by independent oversight authorities and courts within the competent jurisdiction;

(iii) The establishment of one or more independent oversight authorities empowered by law and adequately resourced by the State in order to carry out effective review of any privacy-intrusive activities carried out by intelligence services and law-enforcement agencies;

(b) The adoption of the principle of "if it's exchangeable, then it's oversightable"[17] in relation to any personal information exchanged between intelligence services and law enforcement agencies within a country, and across borders:

[15] European Court of Human Rights, First Section, *Big Brother Watch and Others v. the United Kingdom*, application Nos. 58170/13, 62322/14 and 24960/15, judgment of 13 September 2018.

[16] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf.

[17] Personal data are exchanged between intelligence agencies located in different States on a regular basis, but are not necessarily subject to oversight by the independent oversight agencies located in either the sending or the receiving State. Moreover, certain legislations effectively prevent such oversight or even consultation about the matter between the independent oversight authorities in the sending and receiving States. States are encouraged to amend their laws to empower their

(i) All Member States should amend their laws to empower their independent authorities entrusted with oversight of intelligence activities, specifically and explicitly, with oversight of all personal information exchanged between the intelligence agencies of the countries for which they are responsible;

(ii) Whenever possible and appropriate, the independent oversight authorities of both the transmitting and the receiving States should have immediate, automated access to the personal data exchanged between the intelligence services and/or law enforcement agencies of their respective States;

(iii) All Member States should amend their legislation to specifically empower their national and state intelligence oversight authorities with the legal authority to share information, consult and discuss best oversight practices with the oversight authorities of those States to which personal data have been transmitted or otherwise exchanged by the intelligence agencies of their respective States;

(iv) When an intelligence agency transmits intelligence analysis containing personal information or other forms of personal data received from another State to a third State or group of States, this latter exchange should be subject to the scrutiny of those States' intelligence oversight authorities.

47. The competent authorities in Member States, when contemplating the use of bulk powers for surveillance, should first examine, then prioritize and adopt, to the greatest possible extent, the measures for introducing the good practices recommended in the Stiftung Neue Verantwortung compendium,[18] in addition to applying the criteria for deployment and safeguards adopted by the European Court of Human Rights in *Big Brother Watch and other*s of September 2018.

IV. Right to privacy: a gender perspective

48. The Human Rights Council, in its resolution 34/7, and the General Assembly, in its resolution 71/199, have called upon States "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 adverse effects on women, as well as children and persons in vulnerable situations or marginalized groups."

49. In 1994, the Human Rights Committee, in *Toonen v. Australia*, determined a violation of the right to privacy by the criminalization of consensual same-sex relations between adults. In 2017, the Committee reiterated that the right to privacy covers gender identity (CCPR/C/119/D/2172/2012, para. 7.2).

50. While not an absolute right, the right to privacy is essential to the free development of an individual's personality and identity. It is a right that both derives from and conditions the innate dignity of the person and facilitates the exercise and enjoyment of other human rights.[19] It is a right not restricted to the public sphere.

51. The right to privacy, as a necessary precondition for the protection of fundamental values, including liberty, dignity, equality and freedom from government intrusion, is an

independent oversight authorities to consult with other independent oversight authorities in other States, and follow up on all cases of data exchanged with another State, irrespective of whether they are located in the receiving or sending State, including both raw unprocessed personal data or personal data which is contained in analysis typified by intelligence product. Both types of personal data are exchanged by intelligence agencies and law enforcement agencies, and both should be subject to independent oversight in both the sending and the receiving state.

[18] Thorsten Wetzling and Kilian Vieth, *Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations*, Publication Series on Democracy, vol. 50 (Berlin, Heinrich Böll Stiftung, 2018).

[19] The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized privacy as a gateway to the enjoyment of other rights, see General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8.

essential ingredient for democratic societies, and requires strong protection.[20] The Human Rights Council has adopted resolutions highlighting the interdependent and mutually reinforcing relationship between democracy and human rights.[21]

52. The Special Rapporteur integrates a gender perspective throughout the mandate.[22] Following three successful "Privacy, personality and flows of information" regional consultations, an online consultation entitled "Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations, gender identities, gender expressions and sex characteristics" was undertaken.

53. The full first report of the thematic action stream on privacy and personality is part of a compilation of submissions[23] received by the Special Rapporteur, as well as ancillary research. Apart from the recommendations, the compilation does not necessarily represent the views of its lead author, Elizabeth Coombs, chair of the task force on privacy and personality, nor those of the Special Rapporteur.

Thematic action stream on privacy and personality

54. Submissions on the topic received by the Special Rapporteur advocated an intersectional analysis of economic forces, class, religion, race and gender to identify areas of interest outside the mainstream,[24] and recognition of the interdependency between the right to privacy and democracy.[25]

55. It was reported that individuals' experience of digital technologies and privacy is affected by their gender, together with factors such as ethnicity, culture, race, age, social origin, wealth, economic self-sufficiency, education and legal and political frameworks.[26] The right to privacy was said to be particularly important for those who face inequality, discrimination or marginalization on the basis of their gender, sexual orientation, gender identity, sex characteristics or expression. The Internet, with its reach and relative anonymity, has opened new ways for the interaction and mutual support of lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) people.

56. In submissions, it was recognized that digital technologies have a considerable effect upon privacy by amplifying the experiences of the non-digital world. The benefits of digital technologies were reported as unequally available, owing to structural inequity and discriminatory gender norms that fall heavily upon women, non-binary gender and cis-normative individuals, the poor and minority religious or cultural communities. Cybermisogyny[27] and general cyberabuse of individuals of non-binary gender are enabled by new technologies[28] with infinitely greater reach, durability and impact than previously.

57. The view was strongly expressed in submissions that that does not need to be the case, and digital technology can provide equality in the enjoyment of the right to privacy.

58. In submissions the benefits of smart devices, apps, search engines and social media platforms were recognized, but also their capacity to breach users' privacy according to gender. LGBTQI youth for example, use the Internet more frequently to engage in social

[20] Daniel Therrien, Canadian Privacy Commissioner, Submission to Innovation, Science and Economic Development Canada's national digital and data consultations, 23 November 2018.

[21] Resolutions 19/36 and 28/14 on human rights, democracy and the rule of law.

[22] See www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

[23] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf.

[24] For example, Association for Progressive Communications submission, 2018.

[25] For example, Privacy Commissioner of Canada submission, 2018.

[26] Phoenix Strategic Perspectives, "2016 survey of Canadians on privacy", final report prepared for the Office of the Privacy Commissioner of Canada, December 2016.

[27] West Coast Women's Legal Education and Action Fund (LEAF), *#CyberMisogyny: Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online* (Vancouver, 2014).

[28] Eastern European Coalition for LGBT+ Equality submission, "Gender perspectives on privacy in Eastern partnership countries and Russia", 2018; see also www.ucl.ac.uk/steapp/research/themes/digital-policy-laboratory/gender-and-iot.

media and networking than non-LGBTQI peers and are more likely than non-LGBTQI youth to be bullied or harassed online (42 per cent compared with 15 per cent).[29]

59. Despite the benefits of digital technologies,[30] those most at risk were seen as women, girls, children and LGBTQI individuals and communities,[31] in particular transgender individuals, activists, gay teachers, human rights defenders, sex workers and women journalists.

60. LGBTQI individuals can also experience specific risks, such as "outing", and abuse directly related to their gender identity.[32]

61. It has been found in Canada that social media, while enabling social connections for women and girls, amplifies societal norms by intensifying commercial surveillance; reinforcing existing societal norms and increasing surveillance by family members and peers.[33]

62. Fake accounts on LGBTI dating apps and other social media platforms were reported as being used by State and non-State actors to entrap gay men and arrest or subject them to cruel and degrading treatment, or for blackmail.[34]

63. It was reported that the media, including new media, publish the personal information of LGBTQI people and of human rights defenders, putting their safety at risk.[35]

64. The Internet not only creates contemporary stories but can carry forward in perpetuity those of the pre-digital era, and associated violations of privacy.[36]

65. Some submissions addressed the recognition of gender identity, autonomy and bodily integrity and the expression thereof and expressed their concern for inadequate privacy management in the context of name and gender changes in identity documents.[37] Ordinary, everyday activities requiring identity documents, such as travel, banking, medical appointments, frequently impose deeply embarrassing and distressing privacy incursions for transgender individuals not experienced by individuals of binary genders.

66. The European Court of Human Rights has found States in violation of article 8 of the European Convention on Human Rights for the gender recognition procedures that violate the right to privacy of transgender people.[38]

67. The online availability of public records, judicial notices and decisions concerning gender identity were a privacy concern, in particular in combination with big data and search engine capacity.[39]

---

[29] David Brian Holt, "LGBTIQ teens - plugged in and unfiltered: how Internet filtering impairs construction of online communities, identity formation, and access to health information", 2009.

[30] Submission (name withheld), 2018, citing Valerie Horres, "Online and enabled: ways the Internet benefits and empowers women", *Interface: The Journal of Education, Community and Values*, vol. 10, No. 4 (2010).

[31] 2018 submissions: Kazakhstan Feminist Initiative "Feminita"; Office for the Defense of Rights and Intersectionality; "Stimul" LGBT Group and Transgender Legal Defense Project (Russia); Richard Lusimbo; MPact Global Action for Gay Men's Health and Rights; Transgender Europe; Federatie van nederlandse verenigingen tot integratie van homoseksualiteit; and the International Lesbian, Gay, Bisexual, Trans and Intersex Association.

[32] Gender Perspectives on Privacy in Eastern Partnership Countries and Russia by the Eastern European Coalition for LGBT+ Equality.

[33] Valerie Steeves, and Jane Bailey, "Living in the mirror: understanding young women's experiences with online social networking", in Emily van de Muelen and Robert Heynen, eds., *Expanding the Gaze: Gender and the Politics of Surveillance* (Toronto, University of Toronto Press, 2016). See also https://egirlsproject.ca/ and www.equalityproject.ca/.

[34] Kazakhstan Feminist Initiative "Feminita", submission, 2018.

[35] Ibid.

[36] Osgoode School of Law, confidential submission, December 2018.

[37] Eastern European Coalition for LGBT+ Equality submission, 2018.

[38] European Court of Human Rights, Second Section, *L. v. Lithuania*, application No. 27527/03, final judgment of 31 March 2008; European Court of Human Rights, Fifth Section, *A.P., Garçon and Nicot v. France*, application Nos. 79885/12, 52471/13 and 52596/13, judgment of 6 April 2017.

68. For intersex individuals, privacy intrusions can commence literally from birth, with sex reassignment surgery and hormone treatment to assign a certain sex. "Normalizing" surgery on intersex infants can impact on human rights, including the right to privacy, as it infringes the right to personal autonomy/self-determination in relation to medical treatment. Countries were reported to be responding in a variety of ways.[40]

69. Submissions, including that of the Special Rapporteur on violence against women, referred to the growing body of international, regional and national research on gender-based digital violence.

70. Digital technology and smart devices provide almost limitless ways to harass and control others.[41] Technologically facilitated violence combines issues of gender inequality, sexualized violence, Internet regulation, Internet anonymity and privacy (see A/HRC/38/47).

71. The phenomenon of image-based abuse or "revenge porn" – the sharing of private sexual images and recordings of a person without consent to cause harm – is widely known as a form of online abuse. Research in Australia has found that males and females are equally likely to experience image-based abuse, while people who identified as lesbian, gay or bisexual were more likely to be victims (36 per cent) than heterosexuals (21 per cent).[42]

72. Domestic violence increasingly involves using smart home devices directed at women and dependents[43] which enable new ways to infringe privacy, reduce autonomy and self-determination at home,[44] or in communications.[45] Sometimes legal protections are inadequate[46] or there is a lack of police enforcement of breaches.[47]

73. Cybermisogyny has been manifested on digital platforms.[48] Twitter was reported as the main platform for promoting hate campaigns against women and dissemination of sexual content, while Facebook sees the most attacks on women who defend their rights.[49]

74. Invasions of privacy and online violence are higher for men who do not conform to conventional masculine stereotypes and for lesbian, gay, or bisexual people.[50]

75. The gendered experiences of privacy also affect the enjoyment of other rights, with, for example, women also suffering online censorship and profiling in campaigns targeting female activists and journalists.[51]

Thematic action stream on security and surveillance

76. Surveillance, unless undertaken lawfully, proportionately and necessarily, represents infringements of the human right to privacy. Gender, race, class, social origin, religion,

[39] Kazakhstan Feminist Initiative "Feminita" submission, 2018.

[40] Susan Miller, "California becomes first state to condemn intersex surgeries on children", *USA Today*, 28 August 2018.

[41] Dejusticia submission, September 2018.

[42] Nicola Henry, Anastasia Powell and Asher Flynn, "Not just 'revenge pornography': Australians' experiences of image-based abuse", May 2017.

[43] Makda Ghebreslassie, "Stalked within your own home'': woman says abusive ex used smart home technology against her", CBC News, 1 November 2018; Nellie Bowles "Thermostats, locks and lights: digital tools of domestic abuse", *New York Times*, 23 June 2018.

[44] Bowles, "Thermostats, locks and lights".

[45] Corinne Lysandra Mason and Shoshana Magnet, "Surveillance studies and violence against women", *Surveillance and Society*, vol. 10, No. 2 (2012); Association for Progressive Communications submission.

[46] Bowles, "Thermostats, locks and lights".

[47] Al-Alosi Hadeel, "Cyber-violence: digital abuse in the context of domestic violence", *University of South Wales Law Journal*, vol. 40, No. 4 (2017).

[48] West Coast LEAF, *#CyberMisogyny.*

[49] Women's Institute of Mexico City and Association for Progressive Communications submissions, 2018.

[50] Irish Council for Civil Liberties.

[51] Dejusticia submission, 2018.

opinions and their expression can become factors in determining who is watched in society and make certain individuals more likely to suffer violations of their right to privacy.[52]

77. In a number of countries, gender bias is evident in the higher degree of surveillance of those who identify as members of LGBTQI groups.[53] State surveillance of the LGBTQI community has been facilitated in some countries through legislation. An example given was the Anti-Cybercrime Law enacted in Egypt in 2018.[54]

78. While State surveillance is generally presented as targeting males,[55] counter-terrorism measures have been said to disproportionately affect women and transgender asylum seekers, refugees and immigrants.[56]

79. Women can expect that nearly every detail of their intimate lives will be subject to multiple forms of surveillance by State as well as private actors, from domestic violence to sexual objectification and reproduction.[57]

80. Major platform providers now provide identity management via online identity authentication. Websites, apps and services now require login details and accept identity credentials as authentic following logon via Facebook or Google accounts.[58] Facebook has 60 per cent of this "social log on" market,[59] which provides access to vast amounts of information for the compilation of profiles, enabling insights, in which gender is a variable, into the behaviours of individuals, families, groups and communities.

Thematic action stream on big data and open data

81. The growth in the collection, storage and manipulation of data has increased the possibilities of privacy breaches, which can have different consequences according to gender.

82. Data processing can embed biases relating to gender roles and identities, in particular since data modelling for social intervention increasingly transcends the individual to focus on groups or communities.[60]

83. Data analytics resulting in inferences being made about individuals or groups according to gender, and which lead to discrimination, are contrary to human rights law.

Thematic action stream on health data

84. A particular concern for LGBTQI people is the non-consensual sharing of health data, in particular HIV status.[61] The Grindr app, for example, was found to contain trackers and share personal information, including users' HIV status, with various third parties.[62]

85. Privacy experiences in health-care settings have been found to influence health service usage, with consequent individual and public health impacts.

86. Fears of humiliation or discrimination from loss of privacy can see transgender individuals avoid health services or restrict their use.[63]

---

[52] Mary Anne Franks, "Democratic surveillance", *Harvard Journal of Law and Technology*, vol. 30, No. 2 (Spring 2017).

[53] Association for Progressive Communications submission, 2018.

[54] Joint International submission, 2018; see also George Sadek, "Egypt: President ratifies Anti-Cybercrime Law", Global Legal Monitor, 5 October 2018.

[55] Privacy International 2017.

[56] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/64/211).

[57] Franks, "Democratic surveillance"; Association for Progressive Communications submission, 2018.

[58] "The Economist essay", *The Economist*, Christmas ed., 22 December 2018.

[59] Ibid.

[60] Khiara M. Bridges, *The Poverty of Privacy Rights* (Stanford University Press, 2017); David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (London and New York, Routledge, 2003).

[61] Kazakhstan Feminist Initiative "Feminita" submission, 2018.

[62] Association for Progressive Communications submission, 2018.

87. Violations of women's right to privacy during childbirth can be a powerful disincentive to seeking care for subsequent deliveries.[64]

88. Technologies such as Google Street View, can affect health service usage by women through concerns about being identified using certain health services.[65]

Thematic action stream on use of personal data by corporations

89. There is growing recognition that the private sector has obligations under human rights law as in the Protect, Respect and Remedy Framework proposed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, in 2008 (A/HRC/8/5).[66]

90. Automated decision-making used by digital platforms can produce outcomes affecting genders differently. Legal action, still ongoing, was reported against Facebook for allegedly allowing landlords and brokers to exclude the display of advertisements on the basis of the user's gender.[67]

91. Concern was expressed at the increased number of social media pages and groups promoting violence against women, sexism and harmful gender stereotypes and the amount of community pressure that it took to have such pages removed.

92. It was reported that the following are unknown: how the online platforms make decisions following receipt of online violence complaints; the types and number of cases reported by country; and the actions taken. Amnesty International has found that Twitter failed to adequately investigate reports of violence and abuse and has repeatedly called on the company to release "meaningful information about reports of violence and abuse against women, as well as other groups, on the platform, and how they respond to it."[68]

93. One submission reported positive action by the app Grindr to reduce misuse aimed at entrapment of gay men.[69] However, the common response of digital platforms (Facebook, Twitter, media, etc.) with respect to victims of online gender-based violence was reported as impunity and opacity, with victims generally feeling abandoned.[70]

94. Reports of harm to individuals arising from gender-based technological infringements of the right to privacy included serious, well-documented effects, from fraud, loss of employment and educational opportunities, restrictions on freedom of movement and freedom of association, to dress as one wishes, interference with parenting abilities, loss of reputation and general confidence, violence (even death) and imprisonment, inter alia.[71]

---

63 "New health care clinic for transgender people in pipeline", *Times of Malta*, 7 April 2018.

64 White Ribbon Alliance for Safe Motherhood, "Respectful maternity care: the Universal Rights of Childbearing Women Charter", 2011; and Meghan A. Bohren and others, "The mistreatment of women during childbirth in health facilities globally: a mixed-methods systematic review", *PLOS Medicine*, vol. 12, No. 6 (2015). Dejusticia and Association for Progressive Communications submissions.

65 Melissa L. Davey, "Protect us from anti-abortion protesters, say women's clinics in WA", *Guardian*, 25 January 2018.

66 Internet Rights and Principles Coalition, "The Charter of Human Rights and Principles for the Internet", 2014; Association for Progressive Communications submission, 2018.

67 Consumer Policy Research Centre submission citing article entitled "Money", CNN News, March 2018.

68 See https://decoders.amnesty.org/projects/troll-patrol/findings.

69 Kazakhstan Feminist Initiative "Feminita" submission, 2018.

70 Electronic Media cited in Dejusticia submission, 2018.

71 Association for Progressive Communications Submission, 2018; N. Pushkarna and M.M. Ren, submission 2018; Office of the Privacy Commissioner of Canada, "Online reputation: what are they saying about me?", January 2016; case submissions to Transgender Europe; European Union Agency for Fundamental Rights, *Violence against Women: an EU-Wide Survey – Main Results* (Luxembourg, Publications Office of the European Union, 2015).

95. Experiences of privacy breaches are not homogeneous; infringements can result in increased domestic violence for women and discrimination for LGBTQI people.[72]

96. Invasions of privacy are invasions of the human personality itself and have larger societal impacts. The extreme forms of online abuse and invasions of personal and familial privacy inflicted upon high-profile women discourage girls and women from participating in public roles, thereby undermining women's right to participate in public affairs and affecting the representativeness of democratic institutions.[73]

97. Submissions indicated good practices that protect privacy from a gender perspective, ranging from: legislative reform; gender-neutral, evidence-based policy frameworks; Court decisions; participation of civil society organizations and benefiting from their experience; and gendered privacy community programmes; to educational resources.

98. Good practices for addressing sexual orientation and gender identity privacy issues were seen as being enshrined in the Additional Principles and State Obligations on the Application of International Human Rights Law in Relation to Sexual Orientation, Gender Identity, Gender Expression and Sex Characteristics to Complement the Yogyakarta Principles.[74]

V. Conclusions

99. **The Universal Declaration of Human Rights calls on every individual and every organ of society to promote and respect human rights.**[75] **States, companies, religious bodies, civil society, professional organizations and individuals all have important roles to play.**

100. **The confidence of individuals to share ideas and to assemble is also fundamental to the health of societies and democracy. The loss of privacy can lead to a loss of such confidence, including confidence in government and institutions established to represent the public interests, and to withdrawal from participation, which can adversely impact and undermine representative democracies.**

101. **While privacy rights are not free of cost, or free of risks to Governments, the challenges are outweighed by our collective interest in democracy. The right to privacy for women, as well as children and individuals of diverse sexual orientations, gender identities, gender expressions and sex characteristics, is critically important for all the reasons outlined above and reported in submissions.**[76]

102. **Gender-based breaches of privacy are a systemic form of denial of human rights; discriminatory in nature, and frequently perpetuate unequal social, economic, cultural and political structures.**

103. **Addressing gender-based incursions into privacy requires frameworks at the international, regional and national levels.**

104. **States, in preventing gender-based privacy invasions, need to actively protect privacy in policy development, legislative reform, service provision, regulatory action, support for civil society organizations and educational and employment frameworks, using the experiences of females, males, transgender women and men and intersex people and others who identify as outside the gender binary and cis-normativity.**

[72] Gay, Lesbian and Straight Education Network, *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet* (New York, 2013), in joint international submission, 2018.

[73] Australian Women Against Violence Alliance submission, 2018.

[74] Joint CSO submission, 2018; Peter Micek and Denis Nolasco, "The gender of surveillance: how the world can work together for a safer Internet", Access Now, blog, 6 February 2018.

[75] General Assembly resolution 217 A (III), preamble.

[76] Office of the United Nations High Commissioner for Human Rights, *Born Free and Equal: Sexual Orientation and Gender Identity in International Human Rights Law* (New York and Geneva, 2012).

105. **The protection of personal information online should be a priority, with the adoption of provisions equivalent or superior to the General Data Protection Regulation, for countries that are not party to the Regulation. Gender should be a key consideration for the development and enforcement of privacy protection frameworks.**

106. **Transparency is needed with regard to the way in which private companies use personal data of users,**[77] **and respond to reports of online harassment. Greater gender diversity among those shaping online experiences is important for making products and platforms safer, more socially responsible and accountable.**

VI. Summarized recommendations

107. **With regard to United Nations bodies, all relevant special procedures and other mechanisms of the Human Rights Council and the human rights treaty bodies should integrate gender and privacy into the implementation of their respective mandates.**

108. **It is recommended that Member States:**

(a) **Adopt an intersectional approach that recognizes the specific benefits, experiences and threats to the right to privacy according to gender, and overarching privacy and human rights principles;**

(b) **Undertake an assessment of their legal frameworks for prevention and punishment of privacy breaches based on gender, against relevant laws and treaties at the global, regional and national levels;**

(c) **Adopt policies, legal and regulatory frameworks providing comprehensive protection for the use and development of secure digital communications;**

(d) **Promote meaningful Internet access and bridge any digital gender divide;**

(e) **Take all legislative, administrative and other measures necessary to prevent, investigate and punish breaches of privacy perpetrated on the basis of gender, sexual orientation or gender identity.**

109. **Corporations should implement the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, and avoid infringing the human rights of all persons affected by their practices, with effective consideration of the gender-specific impact of their activities.**

VII. Health data protection

110. Health is the most important fundament of everybody's life. Changes in health status always imply changes in life, many forever. All of us are, at some point in our lives, patients. Situations arise, too, where our health status has a decisive impact on our life. We therefore all have a very legitimate interest in the protection of our dignity and autonomy by the highest available standards in health-data related scenarios.

111. The relationship between a data subject as a patient and a health-care professional is highly sensitive: patients are, by definition, in a vulnerable position. The situation can be distressing and dangerous, with lifelong consequences. The role of a health-care professional requires accurate and complete patient information and processes for using this information in a standardized and transparent manner.

112. The protection of patients (and their genetic relatives) in these moments of existential vulnerability has been subject to legal and ethical considerations and rules for

[77] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (Canberra, Australia, 2018).

millennia. Principles such as medical professional confidentiality, the obligation to establish fully informed consent for treatment, proper documentation of treatment and free choice of treating physician, are some of the fundamental outcomes of centuries of thought on how best to protect the rights of patients.

113. Every medical situation produces personal data. These data are important for treatment purposes and need to be processed following the highest legal and ethical standards. Digitalization is producing more and more medical data, which will be increasingly shared between health-care professionals as they become more and more specialized, and likewise required to collaborate following the highest quality standards.

114. Data processed for health purposes are also important for many other stakeholders and for many different purposes outside the possibly life-changing relationship between the health-care professional and the patient. First, the patient her/himself has a legitimate interest in controlling these data and can consent to their being shared during and after treatment. Second, other stakeholders, such as patients' relatives, institutions to which the patient has an obligation, for example social security institutions, insurance companies or employers, and other, more indirect stakeholders such as medical researchers and the general public, who rely upon an efficient and effective health system, might have an interest in obtaining access to those data.

115. The tensions between these different stakeholders' interests and needs pose very challenging legal and ethical issues.

Critical issues

Informed consent

116. Generally, patients have the right to agree to treatment after being properly informed about possible treatment risks, side-effects and alternatives. The requirements of the consent procedure for medical treatment and medical research are subject to intense, detailed and controversial regulations.

117. Those regulations have not yet been harmonized with the requirements for information provided to data subjects and the validity criteria for informed consent as a legal basis for data processing. Criteria for informed consent are often vague and contradictory.

118. Data subjects can feel overwhelmed by different consent procedures at a time when protection of their data is not their immediate concern. Nor are they always willing and able to understand fully all the implications of the different types of consent that they give. Consent for tests, for treatment, for medical research and for data processing are not clearly distinguished and often have different and possibly conflicting scopes of regulation and different supervisory authorities. This puts patients and their relatives under serious stress, undermining their capacity to freely provide informed consent.

Secondary use for medical research

119. Personal data need to be collected and processed as a basis for medical treatment. They are then stored for reasons of documentation of treatment, sometimes for decades. These data can often also serve as an important source for medical research. There are important arguments that there is an ethical justification (or even necessity) to further use these data for research in the interest of better outcomes for future generations of patients.

120. Research has a different purpose from that of treatment, requiring a different legal basis for the data processing. The requirements of this second legal basis are very diverse and unclear, as many underlying ethical questions are not clearly described or analysed. In particular, questions include whether this secondary use again requires the informed consent of the patient and/or a clearance by a competent ethics committee and/or by supervisory authorities. The issues include personal autonomy arising from bodily privacy and responsibility to the "collective good".

121. If such consent were replaced by another legal basis, further steps would need to be taken to protect the data subject's fundamental rights. Lack of international legislation on

the matter leads to situations in which treating physicians need, or believe they need, additional informed consent from affected patients – consent which in some cases can no longer be obtained, whether for technical or ethical reasons.

Secondary use for other purposes

122. Medical data are of high value also for other purposes, in particular, social security, public health, employment and business. National laws are often silent on data processing for these purposes and it is unclear whether these purposes are ethically and legally justifiable, and which of these secondary uses shall be based either on informed consent or another legitimate legal basis. The purpose binding principle, requiring that secondary use of personal data may only be undertaken for a purpose compatible with the primary purpose is therefore often either ignored or violated.

123. Differences in legislation in this matter lead to a "race to the bottom" in which public services or even businesses reliant on personal health-related information are best served by operating in areas with low levels of data protection.

124. The protection of the data subject's rights – in particular, the right to transparency, including information and access – is problematic, as these secondary uses are undertaken by controllers not known to the data subject and, frequently, for unknown purposes.

Data property as competing means of protection

125. A consequence of the situations described above is that some legal scholars (and even legislators) have begun to argue for a data property right, similar to an intellectual property right, that should alleviate sharing issues with regard to personal and non-personal data. These concepts stand in a very problematic relationship to existing fundaments of data protection and require clear reasoning and justification based on evidence-based predictions of the consequences. Currently, an underlying evidentiary and factual matrix is lacking.

Unclear distribution of responsibilities

126. Medical treatment and research are supervised by regulatory bodies, in particular, ethics committees, consisting of experts and stakeholders, many of them non-lawyers, with no specific expertise in data protection.

127. Many of the requirements formulated by these bodies on data processing for treatment and research, however, are data-protection related, such as specific (and often conflicting) requirements on consent procedures, information to be provided to the patient/data subject, the patient's right to know and not to know, the consequences of withdrawal of consent, etc.

128. The regulations proposed by those bodies may conflict with data protection rules, and their supervision may interfere with supervision undertaken by the data protection supervisors and authorities who are exclusively responsible for monitoring compliance with data protection, such as independent data protection officers and data protection authorities.

Unclear scope of applicability: personal, pseudonymized and anonymous data

129. The basic assumption that data protection laws apply only when data are personal, belonging to a specific individual, is very hard to apply in medical scenarios, as medical data can rarely be fully anonymized. It thus remains very unclear what anonymization measure is "good enough" to keep data outside the scope of data protection legislation.

130. This problem is especially difficult when considering whether medical data should become part of open access/open data initiatives that require the release of (non-personal) data to the public. Data controllers may on the one hand be obliged to keep data under their control for protection of anonymity, but on the other hand obliged to make data freely accessible while risking re-identification. The lack of clarity may facilitate de facto property protection of medical data by data controllers who can – de facto – decide who obtains access to data (anonymized by some method) and under what conditions.

131. The Special Rapporteur stated unequivocally in his 2018 report to the General Assembly that "sensitive high-dimensional unit-record level data about individuals should not be published online or exchanged unless there is sound evidence that secure de-identification has occurred and will be robust against future re-identification."

Lack of data portability and lack of digitalization

132. Medical data are often still collected in an analogue format. Anamneses are often random and incomplete and diagnoses can be based on poor data.

133. The digitalization of medical data, standardization of formats and processes, as well as minimum criteria for data quality, can assist both patients and health professionals to control and responsibly manage health data.

134. States however, tend to establish their own national e-health systems without the participation of citizens and health professionals, and without standardization. This can make data portability impossible for patients and reduce their ability to control their medical data without a standardized instrument enabling secure storage and management of their own health data under their own rules.

Clouds

135. More and more medical information is stored in clouds (like any other data). The consequences are many, inter alia: transfer of personal data across borders with possibly conflicting jurisdictions, lack of control for patients and high-impact security incidents that may affect millions.

136. The minimum requirements for cloud service providers, however, are not harmonized, triggering incentives to operate from areas with a low level of data protection.

Lifestyle products/wearables

137. Health-related data are often no longer (directly) disease-related and are now collected for purposes very different from that of treating or preventing health conditions. In particular, lifestyle-related apps and gadgets ("wearables") collect considerable amounts of health-related data with or without the data subjects' informed consent. They have become increasingly popular, although the legal basis for the collection and requirements for their further use are not clearly defined, no minimum transparency standards apply and the purpose binding principle is not sufficiently taken into consideration.

Security and safety

138. Although health-related data are highly sensitive, and faults in devices processing health data can be potentially life-threatening, there are no clear and specific rules on minimum security and safety standards. The consequence is a series of security and safety incidents with severe impacts for the data subjects affected.

Data breach notification, lack of transparency

139. Although data breaches affecting medical data occur on a regular basis, there are no standards for when and how the data subjects concerned, as well as the general public, need to be informed of such incidents. The situation lacks transparency and fails to meet the accountability standards expected by the public.

Access to justice

140. Non-compliance with data protection legislation can have a life-threatening impact on data subjects. However, from its inception, data protection legislation has lacked effective instruments for enforcement. Unclear rules on competence among data protection authorities, courts, ombudspersons, data protection officers and medical supervisory authorities, as well as uneven distribution of information and knowledge, complexity of regulatory frameworks, make it very hard for data subjects affected to enforce their rights.

141. This lack of enforcement leads to a lack of trust in the medical system and, in particular, the relationship between patient and health-care professional, which can have a detrimental effect on every patient. Minimum standards formulated at the United Nations level are therefore of utmost strategic importance.

Next steps

142. The Special Rapporteur intends to provide guidance for regulating health-related data in order to promote the protection of the right to privacy and the protection of personal data, as provided for in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.

143. Draft guidance[78] containing guiding principles concerning data processing of health-related data emphasizes the importance of a legitimate basis for data processing of health-related data, covering the issues described above. The purpose of the guidance is, first, to serve as a common international baseline for minimum data protection standards for health-related data for implementation at the national level, and second, to be a reference point for the ongoing debate on how the right to privacy can be protected in the context of health data, further developed in conjunction with other human rights (such as freedom of speech, right to a fair trial and protection of property) in a context where medical data are processed and shared globally.

144. The draft guidance, currently before task force experts, is open to public consultation for written comments by 11 May 2019, followed by a public stakeholder meeting in Strasbourg on 11 and 12 June 2019. Member States wishing to participate in this meeting should register their interest by 11 May.

145. A final recommendation of the drafting group, using stakeholders' input, will be provided to the Special Rapporteur and incorporated in his 2019 annual report to the General Assembly in late 2019.

VIII. Privacy metrics

146. The Special Rapporteur is also consulting on "Metrics for privacy".[79] Individuals, civil society and Governments are invited to send their comments and suggestions by 30 June 2019. The intention would be to use such metrics as a standard investigation tool during country visits, both official and non-official.

[78] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf.

[79] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf.