United Nations A/75/147

General Assembly

Distr.: General
27 July 2020

Original: English

Seventy-fifth session
Item 72 (b) of the provisional agenda*
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Right to privacy

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report prepared by the Special Rapporteur of the Human Rights Council on the right to privacy, Joseph A. Cannataci, submitted in accordance with Human Rights Council resolution 28/16.

* A/75/150.

20-10082 (E) 170820

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci

Summary

In the present report, the Special Rapporteur on the right to privacy, Joseph A. Cannataci, proposes a preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic. The evidence base required to reach definitive conclusions on whether privacy-intrusive, anti-COVID-19 measures are necessary and proportionate in a democratic society is not yet available. The Special Rapporteur examines two particular aspects of the impact of COVID-19 on the right to privacy: data protection and surveillance.

COVID-19-related surveillance and contact tracing may take various forms, and could be manual or technological, anonymous or not, consensual or non-consensual. Concerns arise when surveillance apparatus traditionally employed for State security purposes is proposed or hurriedly deployed for a public health purpose to track health data in the context of a pandemic.

If a State decides that technological surveillance is necessary as a response to the global COVID-19 pandemic, it must make sure that, after proving both the necessity and proportionality of the specific measure, it has a law that explicitly provides for such surveillance measures. The law must include safeguards, which, if not spelled out in sufficient detail, cannot be considered adequate under international law.

A more definitive report on the subject is planned for 2021 when more evidence will be available to enable a more accurate assessment.

I. Introduction

1. The privacy dimensions of the coronavirus disease (COVID-19) pandemic are an appropriate and timely subject matter for the present report to the General Assembly, as human rights, including the right to privacy, are severely and, generally, adversely affected by the pandemic. Indeed, responses that are shaped by and respect human rights result in better outcomes in beating the pandemic, ensuring health care for everyone and preserving human dignity.[1]

2. While the priority is to save lives, fighting COVID-19 and respecting human rights, including the right to privacy, are not incompatible. In fact, the trust of citizens that their privacy, for example, is being taken into account builds confidence and willingness to proactively support State measures to prevent the spread of the virus. Human rights can equip States to gain the confidence of their citizenry.

3. The present report constitutes a preliminary assessment as the evidence base required to reach definitive conclusions on whether privacy-intrusive, anti-COVID-19 measures are necessary and proportionate in a democratic society is not yet available. A more definitive report is planned for mid-2021, when 16 months of evidence will be available to allow a more accurate assessment.

4. In the report, the Special Rapporteur addresses two particular aspects of the impact of COVID-19 on the right to privacy: data protection and surveillance. He acknowledges that there are many more privacy issues at stake during the pandemic, including those relating to children, gender, the role of algorithms, among others.

Key points

5. The privacy concerns raised by COVID-19 did not emerge in a vacuum. They manifested themselves in an environment where there were already privacy challenges being addressed by the Special Rapporteur on the right to Privacy, such as surveillance and proper protection of health data.

6. While the COVID-19 pandemic has generated much debate about the value of contact tracing and reliance upon technology that track citizens and those they encounter, the use of information and technology is not new in managing public health emergencies. What is concerning in some States are reports of how technology is being used and the degree of intrusion and control being exerted over citizens – possibly to little public health effect.

7. COVID-19 is a disease and, as a health issue:

(a) The laws concerning public health in several States have long established measures that may be taken to combat communicable diseases, and which provide a standard against which specific COVID-19 measures need to be examined;

(b) The necessary context for considering personal and health-related information in the COVID-19 pandemic should be understood within society's general approach to dealing with health-related data.

8. Privacy-intrusive measures deployed in the name of combating COVID-19, including elements of surveillance, cannot and should not be considered out of context. They should be examined as part of, and consistently with, a holistic comprehensive policy governing surveillance in the respective States.

[1] United Nations, "COVID-19 and human rights: we are all in this together", policy brief, April 2020.

9. Regarding the use of modern technology for checking the pandemic spread, in general, the sub-discipline of privacy engineering has not been given its due importance.

10. Recommendations previously made by the Special Rapporteur, particularly those on Government-led surveillance (A/HRC/37/62) and privacy protection of health-related data (A/74/277),[2] provide guidelines to assist States in addressing the COVID-19 pandemic while respecting their international human rights law obligations.

II. Data protection and surveillance during the COVID-19 pandemic

11. It is useful to consider briefly ordinary pre-COVID public health measures relating to notifiable and communicable diseases.

12. Laws and procedures governing communicable diseases have existed for centuries. They include strict quarantine measures – and quarantine hospitals – to counter pandemics like the bubonic plague. More recently, the role of States in implementing public health responses and processes was illustrated by the United Kingdom of Great Britain and Northern Ireland. Over the best part of two centuries, following John Snow's work on the Broad Street cholera outbreak of 1854 and the increased understanding of the risk of water-borne diseases, the face of public health in the United Kingdom began to change. By 1939, a system of health inspectors had been introduced in the United Kingdom, parts of the British Empire and beyond. Health inspectors at the local level ensured that sanitation laws were enforced – from sewer connections to hand-washing facilities in shops. They were already on the front line against communicable diseases like cholera and tuberculosis before the outbreak of the Second World War which brought about situations, especially crowded unsanitary accommodation conditions, where those contagious diseases could fester more easily. Health inspectors were normally specially trained public officers who had – and still have – strict reporting and notification rules to ensure medical practitioners in the public health department are alerted to outbreaks of serious infectious diseases. The medical practitioners would then take measures to contain and eradicate those communicable diseases.

13. The legal dimension of developments in public health measures included therefore the mandatory communication of information to the public health authorities that a certain type of disease had been identified. That is known as a notifiable disease.

14. COVID-19 is a notifiable disease. In one Member State, it is number 66 on the list of notifiable diseases. Therefore, 65 diseases had already been identified and reported to the national public health authorities.

15. Transfer of sensitive personal data through notification of a communicable disease is an ordinary measure at the national level, but it also has an international dimension. While not extraordinary, transfer of such data can lead to situations where extraordinary measures are invoked.

16. Once notified of the incidence of a disease, public health authorities are granted by law an arsenal of options and measures, ranging from "wait and see" to the strictest

[2] Related appendices and an explanatory memorandum (including extensive unedited versions) to these reports are available at www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

of quarantines. In other words, once they receive health data about a named patient, public health authorities are expected to take an informed decision as to what to do.

17. In most developed countries, health-related personal data is treated confidentially and processed according to needs, including storage for epidemiological purposes. One of the primary purposes of public health authorities is to use epidemiology to prevent and fight epidemics. They have been doing so – generally successfully – even before the era of smartphones and COVID-19. Indeed, there is mounting evidence that, in most developed countries that acted sensibly in a timely manner, as of mid-July 2020, COVID-19 had been successfully fought, and even contained, using time-honoured methodologies without recourse to smartphone-related technologies.[3]

18. Contact tracing is the classic tool used by public health entities to arrest the spread of communicable diseases. It is privacy intrusive because it requires a patient to disclose with whom she or he may have been in contact over a given period of time. Traditionally, in most countries, this has implicitly been one of the exceptional cases where the right to privacy need not be absolute. The need to arrest the spread of a potential epidemic is one of the very few greater goods where public interest is socially valued above the right to privacy or, indeed, other rights such a freedom of movement and freedom of association. Put simply, in order to avoid the spread of cholera or tuberculosis, for example, authorities have the right to: (a) know who is suffering from the disease; and (b) order strict isolation under strict sanitation rules, among other things.

19. All available evidence suggests that there is presently no alternative to, or reasonable substitute for, contact tracing that enables contagion to be arrested, limited and often contained. There is currently no doubt that, wherever practicable, contact tracing works well and that, although privacy intrusive, it can be classified as a necessary measure.

20. Strict and privacy-intrusive manual contact-tracing procedures can also be properly understood as being proportionate to the need to prevent, contain or otherwise fight a public health hazard such as an epidemic. The nature and quantity of personal information required and typically collected in a contact-tracing exercise is that which is strictly necessary to stop the spread of the disease by trying to identify who could also have been infected. Thus, for example, the patient's most comprehensive repository of private information – his or her smartphone – is not accessed or sequestered in the course of traditional contact tracing. Health authorities, often accompanied by police officers enforcing the relevant health law, telephone and/or personally visit people with whom the infected person may have been in contact and enforce the prescribed course of action – often self-isolation for a given period of time.

21. Search and seizure powers have long been linked to the right to privacy. Public health is held to be such a paramount matter of public interest that, in some countries, the ordinary (not extraordinary) search and seizure powers of a public health authority are often greater than those of the police. They are rarely in the news; and the presumption in favour of public health is very much in evidence. Thus, in some States, whereas the search of premises by the police often requires a judicial or executive warrant, the same would not apply if the search is to be carried out under the terms of a public health law, even though the health official may be accompanied by a police officer during such a search.

[3] See, for example, Greece and Malta; if the main criterion/measure of success or failure were the number of deaths per million of population, these countries could be held up as examples of successful handling of the virus without technological surveillance.

A. Extraordinary measures

22. In most States, the relevant law grants the public health authorities the power to take extraordinary measures. This is normally done in the context of a public health emergency, which can be either national or localized, and which must be formally declared in order for extraordinary measures to be invoked. A "public health emergency" is often vaguely defined, if at all, and, in some countries, it can be defined in law as whatever the head of the public health authority decides. There is guidance in, for example, World Health Organization (WHO) definitions.

23. Health emergency powers are huge and can, literally, include anything imaginable (see (g) below) that is "necessary in order to reduce, remove or eliminate the threat to public health".[4] The public health authority may:

(a) Segregate or isolate any person in any area;

(b) Evacuate any persons from any area;

(c) Prevent access to any area;

(d) Control the movement of any vehicle;

(e) Order that any person undergo a medical examination;

(f) Order that any substance or object be seized, destroyed or disposed of;

(g) order such other action be taken as he or she may consider appropriate.

24. When a State grants its public health authorities such wide powers in the case of a public health emergency, the question arises as to whether regular or constant access to a person's computerized device, such as a smartphone, or otherwise monitoring of a person's whereabouts and contacts through geolocation of a smartphone is a necessary and proportionate measure.

25. This also applies in the context where some States have not waited for the existence of a public health emergency to provide a legal basis for access to a person's computerized device. Indeed, in some countries, such access is an ordinary (not extraordinary) power of the health authorities, who may "inspect, extract or seize any record or take any copy of any record relevant to public health in whatever form held and, where any record is kept by means of a computer:

(i) Shall have access to, and inspect and check the operation of any computer, any associated apparatus or material which is or has been or could have been used in connection with the records;

(ii) Shall require any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material to afford him [or her] such assistance as he [or she] may reasonably require".[5]

26. Such provisions are arguably aimed at providing targeted access in a normal situation and not on the scale of large percentages or all of the population of an entire State, as has been contemplated, tested and/or deployed during the COVID-19 crisis to date.

[4] Malta, Public Health Act, Chapter 465 of the Laws of Malta, art. 15.

[5] Ibid., art. 6(1)(c).

B. Regulations for health-related data and privacy

27. COVID-19-related data is health data and is the first category of personal data to qualify for special levels of protection. The protection of health data can be said to be the pioneer of data protection rules and regulations. The Hippocratic Oath – thought to date to between the sixth and third centuries B.C. – requires physicians to preserve the secrecy and confidentiality of their patients' medical information.[6]

28. Every medical situation inevitably generates personal data that requires processing at the highest legal and ethical standards. The debate on privacy in the United States of America, in 1973, included the first health data principles, whereas in Europe, the Council of Europe's first ever recommendation on data protection, in 1980, concerned medical data, predating the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of January 1981. The Council's recommendation has since been revised twice (in 1997 and in 2019).

29. The digitalization of data has resulted in significant growth in the volume of health-related data processed and in more complete patient profiles. Digitalization has not only increased the quality of the data, but has also made it easier for the data to be shared among health-care professionals, thus enhancing the potential to improve the provision of health care.

30. The individual to whom the data relates has a manifest interest in the data and in controlling it. That individual's relatives, third parties in transactional relationships with the individual and other indirect stakeholders, such as the individual's community, the general public and medical researchers, also have an interest in that individual's data. The interests are various, varied and unequal, and hence various specific provisions to ensure the deserved respect for the right to privacy are merited, in accordance with article 12 of the Universal Declaration of Human Rights.

31. The pool of indirect stakeholders interested in health-related data has grown exponentially in recent history, and that growth is equally reflected in the tensions among the different stakeholders, resulting in increasingly challenging legal and ethical issues.

32. Both European Union General Data Protection Regulation[7] and Council of Europe Convention 108[8] recognize health data as a "special category of data". According to the Convention, the processing of health data is permissible only where appropriate safeguards are enshrined in the law. While the Regulation provides more scenarios in which health data may be processed, the processing of health data, as opposed to more generic personal data, remains subject to increased restrictions. The Regulation permits European Union member States to "maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."[9]

[6] Institute of Medicine, *Health Data in the Information Age: Use, Disclosure, and Privacy* (Washington, D.C., National Academies Press, 1994).

[7] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, art. 9(1).

[8] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 1981, art. 6.

[9] European Union, General Data Protection Regulation, art. 9(4).

33. In March 2019, the Committee of Ministers of the Council of Europe adopted Recommendation CM/Rec(2019)2 on the protection of health-related data.[10] It contains a set of principles intended to protect health-related data, incorporating both the provisions of Convention 108 and the additions introduced in the 2018 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, known as Convention 108+, which were intended to ensure that the Convention responded to the new challenges in the digital era. [11]

34. In October 2019, the Special Rapporteur formally submitted to the General Assembly the Recommendation on the protection and use of health-related data (A/74/277, annex). The Recommendation recognizes the sensitivity and high commercial value of health-related data, and provides a common international baseline for minimum standards of protection for health data.[12] It is intended to complement existing regulations and recommendations, while taking into account the increasing digitalized processing of individuals' health data. It addresses lacunae and uncertainties that were brought about by the introduction of electronic health records, mobile applications, targeted marketing, employers' and insurers' access to health-related data, and the data protection needs that are particular to specific groups of society, such as persons with disabilities and refugees.

35. The Recommendation is evidence of how data protection safeguards have evolved over time to keep up with societal and technological advancements. Whenever international crises have arisen – no less those caused by global pandemics – existing rules and recommendations were put to the test. Reasons of public health have always provided, and still do, a legitimate legal basis for the processing of personal data and health-related data, with the aim of fighting and containing the spread of a pandemic. The Recommendation specifies that the processing of health-related data is legitimate when it is carried out in the public interest and with adequate safeguards, especially in the form of security and organizational measures, put in place.[13]

36. Individuals' health-related data have become a key tool used by Governments and scientists worldwide in the fight against the continued spread of COVID-19. A number of Governments, and often their respective law enforcement agencies, are processing health-related data (sometimes coupling it with other personal metadata,[14] such as location data) with a view to, inter alia, enforcing quarantine or self-isolation obligations, and/or to feed into research aimed at shaping required restrictive measures on social interaction. In some instances, entities with access to those sensitive personal data are newly emerged indirect stakeholders, and their sudden emergence may have come at the expense of coherent policies that safeguard the privacy and integrity of health-related data.

37. One way in which Governments and technology companies are processing health-related data in the fight against the COVID-19 pandemic, is by using technology to track individuals who have tested positive for the disease, and by

[10] See https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html.

[11] Council of Europe, "Protection of health-related data: Council of Europe issues new guidelines, press release (March 2019). Available at www.coe.int/en/web/portal/-/health-related-data-council-of-europe-issues-new-guidelines.

[12] A/74/277, annex, para. 4.1 (c).

[13] Ibid, para. 4.1 (f).

[14] Privacy International defines metadata as "any set of data that describes and gives information about other data such as the timestamp of an electronic message, the name of the sender, the name of a recipient, the location of the device, etc." See "Extraordinary powers need extraordinary protection", 20 March 2020. Available at https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections.

extension, every individual with whom they may have come into contact. This technological extension of the traditional process of contact tracing is often done through the processing of data generated by mobile phones, and is an approach that has been tested in the control of previous pandemic crises, for example, in 2014, in the management of the spread of the Ebola virus in West Africa, and in 2015, in the fight against the Middle East respiratory syndrome (MERS).[15] Today, more than ever, and especially in the light of more widespread mobile phone use, this contact-tracing method has the potential to equip Governments and their respective public health authorities to successfully control the risk posed by pandemics, such as COVID-19, as well as to monitor the long-term spread and evolution of a disease. The processing of individuals' health-related data merits the development of appropriate regulation modelled on the Special Rapporteur's Recommendation on the protection and use of health-related data, and which should be enshrined in the national legislation of States.

38. The Recommendation offers the necessary guidance to States electing to legislate for secure processing of health-related data, even in the unprecedented global scenarios brought about by COVID-19. Every indirect stakeholder is included within the scope of the Recommendation, as its applicability is not limited to medical and health professionals, but rather encompasses the "data processing of health-related data in all sectors of society, including the public and private sectors".[16] It requires all controllers and processors to take all appropriate measures to fulfil their obligations with regard to health-related data, and to be able to demonstrate to a competent supervisory authority that all the respective data processing is indeed being carried out in accordance with applicable obligations.[17] That requirement further echoes the call for States to set up independent oversight authorities that are equipped to monitor the implementation of the necessary surveillance, even epidemiologically oriented surveillance, as will be explained below. A very rough count carried out by the mandate holder suggests that, at best, less than 60 States partially meet the minimum standards set out in the Recommendation. In other words, more than 70 per cent of United Nations Member States are not even close to meeting those standards. A key question that a concerned citizen needs to ask, therefore, is: To what extent, if at all, does my country effectively enforce the standards set out in the Recommendation on the protection and use of health-related data?

39. It should be noted that Convention 108+ requires that, "even in particularly difficult situations, data protection principles are respected."[18] It is important to be aware that States are duty bound to protect the health of their citizens, but also to equally protect their right to privacy, both in the short-term measures taken, as well as in the long-term planning. The two do not contradict each other and States are encouraged to refer to the Recommendation as a blueprint for the rules and legislation that would provide the appropriate legal basis for the processing of health-related data, even where this may exceptionally involve an element of surveillance.

40. One year after the formal submission of the Recommendation to the General Assembly, and in the midst of a health-related crisis such as COVID-19, there is need for urgent action to remedy the current low levels of compliance with the standards set out in the Recommendation.

---

[15] Privacy International, "Extraordinary powers need extraordinary protections", 20 March 2020.

[16] A/74/277, annex, para. 2.1.

[17] Ibid., para. 4.5.

[18] Council of Europe, "Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe", 30 March 2020. Available at https://rm.coe.int/covid19-joint-statement/16809e09f4.

C. Surveillance and health-related data

Surveillance by law enforcement, intelligence and security agencies

41. The mandate of the Special Rapporteur on the right to privacy was created in 2015 in direct response to the revelations by Edward Snowden about State-led surveillance. After more than two years of wide consultation, in March 2018, the Special Rapporteur submitted to the Human Rights Council a draft legal instrument[19] on surveillance carried out by law enforcement agencies and security and intelligence services.

42. The document outlines many of the basic principles and minimum measures (safeguards and remedies) that a State should respect or introduce to comply with article 11 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. As leading regional courts have pointed out,[20] an element of surveillance in modern society is permissible provided that surveillance measures are provided for by law and are necessary and proportionate in a democratic society. If such surveillance is carried out, it should be clear that the key safeguard is efficient and timely oversight of such surveillance.

43. The minimum standards recommended as being essential include the existence of an independent authority responsible for oversight *ex ante* and *ex post* of all surveillance measures taken by both law enforcement agencies and intelligence services. The national law of each and every State, therefore, should entrench effective oversight of both law enforcement agencies and security and intelligence services, by properly resourced and independent oversight authorities. As confirmed by the jurisprudence of both the European Court of Human Rights and the European Court of Justice, surveillance should preferably be targeted and always conducted in a proper way, with prior authorization from an independent external authority, preferably, but not necessarily, comprising at least one person of judicial standing.

44. The vast majority of States are very far from achieving those standards. As of July 2020, of the 193 States Members of the United Nations, only a tiny minority (less than 10 per cent), was anywhere close to meeting the standards necessary for a Government to ensure that the privacy of citizens is properly protected and respected when it comes to State-led surveillance.

45. The COVID-19 picture is complicated further when surveillance apparatus traditionally employed for State security purposes is proposed or hurriedly deployed for a public health purpose such as combating COVID-19.

46. For individuals to be protected from interference with their right to privacy, their Governments should be subject to regulatory procedures provided for by national laws. States should include in their laws precautionary measures designed to ensure that surveillance cannot be initiated until, or unless, it is proven to an independent and competent authority that such surveillance is legal, necessary and proportionate to the objective pursued, that is, "solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society".[21]

47. The Special Rapporteur has recommended also that States complement those measures by incorporating into their domestic legal system the standards and

[19] See Working draft legal instrument on Government-led surveillance and privacy. Available at www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

[20] See European Court of Human Rights, *Big Brother Watch and others v. The United Kingdom* (applications Nos. 58170/13, 62322/14 and 24960/15), judgment of 13 September 2018.

[21] Universal Declaration of Human Rights, art. 29(2).

safeguards set out in Convention 108+, especially article 11, and that any personal information exchanged between intelligence services and law enforcement agencies within and across borders be subject to oversight by their national independent authorities.

48. All States are encouraged to introduce into their domestic legal system or to update a detailed law on surveillance by law enforcement agencies and security and intelligence services with oversight safeguards, so as to provide the legal basis for surveillance measures that are necessary and proportionate in a democratic society, and in full compliance with article 9 of Convention 108 and article 11 of Convention 108+. The Special Rapporteur has sought to encourage increased awareness and exchange of good practices in oversight of surveillance through the creation of the International Intelligence Oversight Forum, which has met annually since 2016. States are urged to engage with peers and participate actively in the Forum.

Surveillance in epidemiology – a tool to fight the spread of diseases

49. In the course of their studies, epidemiology students, as opposed to privacy lawyers, would learn that surveillance is defined as "the continual scrutiny of all aspects of occurrence and spread of a disease that are pertinent to effective control", and that it involves the "systematic collection, analysis, interpretation, and dissemination of health data". Disease detection and diagnosis is "the act of discovering a novel, emerging or re-emerging disease or disease event and identifying its cause." Diagnosis is "the cornerstone of effective disease control and prevention efforts, including surveillance".[22]

50. Surveillance in the context of epidemiology has always been considered as key to effective control of the spread of a disease. Such surveillance includes information relating to medical data, such as clinical diagnoses, mortality rates, as well as other relevant information necessary to detect and track the disease, in terms of person, place and time. That approach[23] was particularly strengthened with the spread of HIV/AIDS, hepatitis C and dengue haemorrhagic fever.

51. With every single country playing a role in the spread of epidemics, national reporting systems relating to the spread of infectious diseases are laid down within the legal frameworks of various countries, typically as outlined above.

52. WHO has a mandate to lead and coordinate global surveillance for such reporting. The International Health Regulations (2005) constitute a legally binding agreement with 196 countries, including all WHO member States and some non-member States. Signatory States are bound to report any event that may constitute "a public health emergency of international concern". Such an emergency is defined as "an extraordinary event which is determined … (i) to constitute a public health risk to other States through the international spread of disease, and (ii) to potentially require a coordinated international response".

53. The broad notification requirement therefore extends the scope beyond notifiable or communicable diseases, and is aimed specifically at successful early detection of all public health events that could have grave international consequences. Notably, the Regulation recognizes specific diseases that are considered to raise particular concern, and obliges signatories to the Regulation to immediately notify

[22] Institute of Medicine, *Global Infectious Disease Surveillance and Detection: Assessing the Challenges–Finding Solutions, Workshop Summary* (Washington D.C., National Academies Press, 2007).

[23] The "Spanish flu" pandemic of 1918–1919 is estimated to have killed some 40 million people worldwide. It brought home the need for effective public health surveillance aimed at detecting and preventing such pandemics.

WHO of any single case of certain diseases, inter alia, severe acute respiratory syndrome (SARS), irrespective of the context in which it occurs.

54. WHO data sharing during a public health emergency "permits analyses that allow the fullest possible understanding of the emergency, with a view to ensuring that decisions are based on the best available evidence". Different considerations are given for each of the following three categories:

(a) surveillance, epidemiology and emergency response, including health facilities,

(b) genetic sequences, and

(c) observational studies and clinical trials.[24]

55. States parties to the International Health Regulations are encouraged to share data with the aim of preventing the spread of any global pandemic, and WHO commits to only publishing anonymized data. Such published data would include data from surveillance and monitoring, as reported by States parties, as well as from the emergency response of the respective State. One example of such a response would be contact tracing and details pertaining to treatment. The published data may also include information on medical facilities, including their location and resources. Article 45 of the Regulation sets out the protection requirements for such data, including the removal of any personal identifiers and locations.

56. The WHO Report on Global Surveillance of Epidemic-prone Infectious Diseases lists the types of surveillance data that are generally collected and reported with regard to infectious diseases. One of the surveillance methods reports information pertaining to the confirmation of cases seen in health services. This is known as passive surveillance since it amounts to reporting cases that have not been actively sought out. Another method is the surveillance of disease strains. Some diseases, such as influenza, have new strains occurring frequently. Another report is generated by population screening, which involves actively and systematically screening the population to find cases of the disease in the community.

57. Therefore, the practices of surveillance, monitoring and contact tracing are not new concepts in informing epidemiology. WHO makes reference to such measures with a view to protecting populations from the spread of any epidemic.

58. WHO lists some of the objectives of COVID-19 surveillance as being to:

(a) Enable rapid detection, isolation, testing and management of suspected cases;

(b) Identify and follow up contacts;

(c) Guide the implementation of control measures;

(d) Detect and contain outbreaks among vulnerable populations;

(e) Evaluate the impact of the pandemic on health-care systems and society;

(f) Monitor longer term epidemiologic trends and evolution of COVID-19 virus;

(g) Understand the co-circulation of COVID-19 virus, influenza and other respiratory viruses.[25]

[24] WHO, "Policy statement on data sharing by the World Health Organization in the context of public health emergencies", 13 April 2016.

[25] WHO, "Surveillance strategies for COVID-19 human infection", Coronavirus (COVID-19) update No. 29, 5 June 2020.

59. The objectives outlined above can potentially be justified under the heading of public health or public interest, and are likely to constitute a legal and justifiable reason to process health-related data, but only if and insofar as they are processed in accordance with data protection legislation enacted in line with the Special Rapporteur's Recommendation on the protection and use of health-related data.

60. Surveillance for epidemiological purposes, as listed above, can take many shapes and forms, but must be necessary and proportionate to the objectives to be achieved. The above-listed objectives could be used as a guide for States to identify their objectives.

D. Technology and health-related data – privacy and public health considerations

Legal basis for ordinary/extraordinary measures and need for a measured proportionate response

61. As mentioned above, international treaties and most national Constitutions contain provisions that allow States to temporarily increase their powers during a period of crisis. Governments can make use of special powers, which would normally be considered infringements or violations of fundamental human rights and freedoms, during a limited period of time and for a specific purpose – normally to fight or prevent an imminent threat (in this case, to prevent the spread of COVID-19).

62. States have various ways of making use of enhanced powers, depending on the provisions of their Constitution and/or ratified international treaties. Some States may call it a "state of emergency", others, a "state of necessity", while, especially during the current COVID-19 crisis, still others have declared a "public health emergency". Each special temporary legal regime awards different powers to the authorities. For example, research to date indicates that at least 15 States in the global North[26] have declared a state of emergency in response to the current crisis.

63. In a statement[27] issued at the beginning of the crisis, a group of Special Procedures experts underlined the importance for States to find the right balance between the extraordinary measures put in place to fight the spread of COVID-19 and the protection of human rights. Extraordinary measures are – or should be – strictly defined by national laws and Constitutions as legal orders of specific form issued by the authorities equipped with special powers in a state of emergency. They are also recognized in international legal instruments, including the International Covenant on Civil and Political Rights (art. 4) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 15).[28]

[26] Time limit for the submission of the present report permitted only an outline analysis of a few countries where reliable data was more readily available. Over the period June 2020 to June 2021, the Special Rapporteur intends to gather and triangulate data that would permit a more accurate and reliable picture of the COVID-19-related legal and operational measures available and deployed in the global South. The COVID-19 situation in Asia, Africa and South America, for example, is still very much an emerging one that is being constantly monitored by the mandate holder, who intends to report thereon in his next annual report.

[27] OHCHR, "COVID-19: States should not abuse emergency measures to suppress human rights – UN experts", press release, 16 March 2020. Available at www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E.

[28] See also, European Court of Human Rights, *Lawless v. Ireland (no. 3)*, judgment of 1 July 1961, para. 3; and *Denmark, Norway, Sweden and the Netherlands v. Greece* (application Nos. 3321, 3322, 3323, 3324/67, Report of the European Commission of Human Rights of 5 November 1969.

64. The importance of adequately coordinating the measures taken to prevent large-scale contagion of COVID-19 with respect for fundamental human rights, including the right to data protection, is very well addressed in the joint statement issued by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe on 30 March 2020.[29] Surveillance, tracking measures and similar restrictions to basic freedoms have been applied in the context of public security. As a result, there is a non-negligible corpus of experience amassed in favour of reconciling national security with fundamental rights by ensuring that privacy-intrusive measures are provided for by law and necessary and proportionate in a democratic society. However, transferring that experience to the field of public health might not be as straightforward, and certain adjustments towards an appropriate, data privacy- and data protection-sensitive approach might be necessary.

65. Nearly 30 per cent of States Members of the United Nations have already formally committed under international law to respect the principles of necessity and proportionality: the 55 States that have ratified the Council of Europe Convention 108 or Convention 108+ are already bound by article 9 of Convention 108 or article 11 of Convention 108+. They should be well aware that measures taken in the interest of public health must meet the same tests of legality, necessity and proportionality in a democratic society as provided for in the above-mentioned articles. For the purposes of the present report, the COVID-19 situation is understood as being covered under article 11, paragraph 1, subparagraph a, of Convention 108+, under "other essential objectives of general public interest". A first step for the other 70 per cent of Member States that are not parties to the Convention would therefore be to avail themselves of the Special Rapporteur's earlier recommendation and accede to Convention 108+ at the first opportunity, then put in place all the mechanisms identified herein and elsewhere, and apply its principles to everyday governance, including the protection of health-related data.

66. Thus, where a State has a law that provides for extraordinary powers, and where any measures deployed when exercising such powers seem to be privacy invasive, including any form of surveillance (e.g., geolocation, proximity monitoring, malware, telephone tapping, profiling), they should require oversight *ex ante* and *ex post* to prove that they are necessary and proportionate to the pursued objective. In that way, it would be guaranteed that only the appropriate surveillance method is carried out, by the appropriate people, for the appropriate purpose and for the appropriate length of time.

E. Technology and other realities

67. Among the various technological means that Governments have turned to in response to the COVID-19 pandemic, smartphone applications have been one of the most discussed and/or deployed methods used by States to monitor the spread of the virus. So far, many countries seem to have taken the decision to develop their own

[29] Council of Europe, "Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe", Strasbourg, 30 March 2020. Available at https://rm.coe.int/covid19-joint-statement/16809e09f4.

contact-tracing applications. Therefore cross-border interoperability is still only a desire and a recommendation for the future.[30]

68. Some aspects taken into consideration in developing contact-tracing applications include:

(a) How the application gathers information on the location/proximity of individuals (e.g., some applications identify a person's contacts by tracking the smartphone's movements, using the Global Positioning System or triangulation from nearby cellular towers), and looks for other smartphones that have been in the same location at the same time;

(b) The use of proximity tracking, in which smartphones swap encrypted tokens with other nearby smartphones over Bluetooth signal, which handles the information gathered and its storage (i.e., centralized versus decentralized approaches);

(c) Whether installation and use of the application is voluntary or mandatory (i.e., consensual versus non-consensual deployment).

69. Many applications rely on the joint application programming interfaces developed by Apple and Google. The interface allows iOS and Android smartphones to communicate with each other via Bluetooth, which enabled the developers to build a contact tracing application that will work for both. The two companies plan to build this capability directly into their operating systems.

70. One of the most serious problems, in general, is that the sub-discipline of privacy engineering is not given its due importance. The bigger technology companies (such as Apple) were among the first to introduce privacy engineering as a dedicated disciplinary approach. It is important to emphasize that sole reliance on legal safeguards is not enough. Privacy should be considered from the very beginning, starting with the engineering of the application. Although that is accounted for in the spirit of the "Privacy by Design" approach advocated in the European Union General Data Protection Regulation, the reality of privacy engineering is nowhere near such lofty ideals. In practice, the vast majority of the world's countries are served by information and communications technology engineering teams for whom performance or functionality – not privacy – lies at the core of the engineering process. The paucity of privacy engineering training and research in universities means that it will take several years, possibly decades, for the situation to change to one where privacy by design becomes a reality.

71. There is some hope, however, in concerted action by tiny groups of motivated individuals. A promising practice developed in response to the COVID-19 situation is Decentralized Privacy-Preserving Proximity Tracing, an open protocol developed by a group of engineering schools[31] for Bluetooth-based tracking in which the contact logs of an individual's smartphone are only stored locally, therefore no central authority can know who has been exposed. A number of States (such as Austria, Estonia, Germany and Switzerland) have announced that the applications they have

[30] It should be stressed that, while all efforts have been made to ensure the accuracy of the information provided, the COVID-19 situation has put serious constraints on the ability of the Special Rapporteur to triangulate data, especially data gleaned from media reports. The information contained in the present report regarding current practices or responses in various States is therefore offered as possibly indicative, and not necessarily definitive. It is expected that this information will, COVID-19 permitting, be adequately verified and reflected in a report in 2021.

[31] École Polytechnique Fédérale de Lausanne, ETH Zurich, KU Leuven, Delft University of Technology, University College London, Helmholtz Centre for Information Security, University of Torino and ISI Foundation.

deployed at the national level are based on this protocol. By comparison, Pan-European Privacy-Preserving Proximity Tracing – another protocol developed in response to the COVID-19 pandemic by a consortium of academics and business actors – lacks certain transparency and privacy-preserving characteristics (e.g., user data is stored on a server, while Decentralized Privacy-Preserving Proximity Tracing has a decentralized capability so that data never leave the user's smartphone).

72. Depending on the design of the application, health officials may not be able to have access to data on persons to whom an infected person has been in proximity. Some applications (e.g. COVIDSafe (Australia) and StopCovid (France)) have a centralized design, which means that the infected person must upload the identification of his or her smartphone and that of the smartphones of their recent contacts to a central server. Although the identifications are anonymized, officials can see the entire network of contacts.

73. Other applications (e.g., in Germany) are decentralized, meaning that data about a person's recent contacts stay on the person's smartphone. An infected person uploads only his or her own anonymized identification to a central database; any person who has the application on his or her smartphone can regularly upload the list of infected users and check for smartphones to which they have been in proximity recently. Privacy advocates see big advantages in this design and argue that it does not leave data about users' social networks vulnerable to hacking or exploitation.

74. The importance of smartphone data to medical research is also relevant and should be taken into consideration, as it is a reason broadly invoked by States that choose the centralized design. In the case of decentralized applications, national public health departments and researchers only learn about people who actually call in to report that they have received a notification. Since the public health actors do not have access to the smartphone numbers of the people who have been notified and who have not reported a notification, it could be harder to evaluate the accuracy and precision of the data captured by the application.

75. There is an essential difference between the way applications are being promoted or enforced. Most States encourage citizens to download the application voluntarily, with the user's free consent; India is the only democracy that has made downloading the application mandatory for millions of people. In some rare, but important, cases, the deployment of the application has been deemed obligatory for certain categories of individuals, for example, in the Republic of Korea, or even for anybody enjoying a normal life, such as the experience in China.

76. Even when installing the application is "voluntary", compulsory data entry varies and it is important to assess the level of data protection by ensuring that only necessary information is captured by the application, storage of the data respects international data protection standards, and such storage is limited in time and used only for the right reasons.

Hybrid systems of surveillance

77. The method of surveillance applied in the Republic of Korea incorporated the use of a smartphone application, but did not rely on it alone; rather, it used a hybrid approach bringing together technologies used conventionally in law enforcement and counter-terrorism, and combining several sources of personal data to build a picture of a person's movements, including:

– Credit and debit card transactions – which can show where a person has shopped or eaten, and how they have travelled across a transport network;

– Phone location logs obtained from mobile operators – which give a rough idea of which neighbourhood a person is in as they connect to different phone masts;

– Details captured by the extensive network of surveillance cameras.[32]

78. The system used in Israel is not only modelled on counter-terrorism technologies but uses them directly. It has been reported that, since mid-March, the Israeli Security Agency has been assisting the Government of Israel in conducting epidemiological investigations by providing the Ministry of Health with the routes of coronavirus carriers and lists of individuals with whom they have been in close contact.[33] That information is available from the communication metadata database of the Agency. The surveillance method used in Israel is particularly interesting given that the Supreme Court of Israel had invalidated its use in April 2020, compelling the Government to pass a new law to provide the correct legal basis for such surveillance. Although, since March, the Government of Israel has tried to strengthen the level of parliamentary scrutiny of its intelligence operations, unlike the Netherlands, the United Kingdom or other countries, it does not possess an independent statutory "expert body" that is capable of acting as a completely independent oversight authority to complement the work of the Parliamentary Committee.

III. Conclusions

79. **COVID-19-related surveillance and contact tracing may take various forms, and could be manual or technological, anonymous or not, consensual or non-consensual.**

80. **In order to properly assess COVID-19 measures, it is important to ensure that they are moderately useful or indispensable, or not useful at all. This assessment would help to determine whether the measure is necessary and proportionate in a democratic society, and thus permissible under international privacy law.**

81. **It is far too early to assess definitively whether some COVID-19-related measures might be unnecessary or disproportionate. The Special Rapporteur will continue to monitor the impact of surveillance in epidemiology on the right to privacy[34] and report to the General Assembly in 2021. The main privacy risk lies in the use of non-consensual methods, such as those outlined in the section on hybrid systems of surveillance, which could result in function creep and be used for other purposes that may be privacy intrusive.**

82. **Intensive and omnipresent technological surveillance is not the panacea for pandemic situations such as COVID-19. This has been especially driven home by those countries in which the use of conventional contact-tracing methods, without recourse to smartphone applications, geolocation or other technologies, has proven to be most effective in countering the spread of COVID-19.**

83. **If a State decides that technological surveillance is necessary as a response to the global COVID-19 pandemic, it must make sure that, after proving both**

[32] Rory Cellan-Jones, "Tech Tent: Can we learn about coronavirus-tracing from South Korea?" *BBC News*, 15 May 2020. Available at www.bbc.com/news/technology-52681464.

[33] Amir Cahane, "Israel reauthorizes Shin Bet's coronavirus location tracking", *Lawfare*, 03 July 2020. Available at www.lawfareblog.com/israel-reauthorizes-shin-bets-coronavirus-location-tracking.

[34] The Special Rapporteur is in the process of compiling tables containing basic data on the use of technology in relation to COVID-19, which will be updated to reflect the most accurate information. The tables will be posted as an appendix to the present 2020 report to the General Assembly on the mandate holder's website (www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx) and updated as necessary.

the necessity and proportionality of the specific measure, it has a law that explicitly provides for such surveillance measures (as in the example of Israel).

84. **A State wishing to introduce a surveillance measure for COVID-19 purposes, should not be able to rely on a generic provision in law, such as one stating that the head of the public health authority may "order such other action be taken as he [or she] may consider appropriate". That does not provide explicit and specific safeguards which are made mandatory both under the provisions of Convention 108 and Convention 108+, and based on the jurisprudence of the European Court of Human Rights. Indeed, if the safeguard is not spelled out in sufficient detail, it cannot be considered an adequate safeguard.**

85. **WHO maintains a list of COVID-19 cases (and deaths) by WHO region.**[35] **The list serves as a constant reminder to prioritize the adoption of measures which would significantly reduce deaths. Put simply, if a State wishes to use a privacy-intrusive measure, especially one that can easily be abused, such as technological surveillance, the State must demonstrate that the measure is necessary and proportionate to achieve the pursued objective. The State concerned must put the measure to the strict test by asking the following questions: Was/is there another method that could be used that would have avoided the deaths to the same extent as or better than the privacy-intrusive technology deployed or contemplated? Was/is the technology deployed "an easy way out"? What is the cost – to privacy or financially – of deploying the particular technology? It is only then that the necessity and cost of privacy-friendly measures can be properly assessed, and the assessment of proportionality can be done.**

86. **It is understandable that some of the States that have adopted privacy-intrusive technologies to combat COVID-19 are claiming that they have tracked a certain amount cases and/or have avoided a certain amount of deaths. However, those claims are yet to be verified. It is still too early to adequately assess the efficacy of the COVID-19-related measures taken, and to provide answers to the following questions:**

(a) **What works?**

(b) **What works best?**

(c) **What works best for whom?**

(d) **What works best where?**

87. **Once the measure is identified, the next question is: Why did/does this measure work best, for whom and where? It is hoped that the evidence produced over the next 12 months will enable a better understanding of these and other variables, which would help privacy experts to properly assess the COVID-19 measures deployed, and determine whether the non-consensual measures meet the strict tests of proportionality and necessity.**

---

[35] WHO, Coronavirus disease (COVID-19), Situation report. Available at www.who.int/docs/default-source/coronaviruse/situation-reports/20200712-covid-19-sitrep-174.pdf?sfvrsn=5d1c1b2c_2. It should be emphasized that, at this stage, it is far from clear as to whether efficacy in death reduction should be the sole or main yardstick for an anti-COVID-19 measure. Further consultation is required to determine this.