United Nations A/76/220

General Assembly

Distr.: General
23 July 2021

Original: English

Seventy-sixth session
Item 75 (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 on the right to privacy, Joseph A. Cannataci, submitted in accordance with Human Rights Council resolution 28/16.

* A/76/150.

21-10203 (E) 180821

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, aims to shed further light on how pandemics can be managed with respect to the right to privacy. It is a more definitive analysis building on the report of the Special Rapporteur to the General Assembly in 2020 (A/75/147) now that there is greater evidence available to allow a more accurate assessment of the ongoing coronavirus disease (COVID-19) pandemic. The Special Rapporteur examines in particular the impact of measures to combat COVID-19 on data protection, technology and surveillance and notes that ongoing measures taken by States to control the spread of COVID-19 continue to negatively impact the enjoyment of the right to privacy and personality and other interrelated human rights. The report contains recommendations to State and non-State actors for strengthening privacy and personality; safeguard children's access to online education; protect informational privacy; and ensure transparency and metrics.

I. Introduction

1. Although the coronavirus disease (COVID-19) pandemic is still evolving, more material is now available to indicate how ongoing pandemic management can better incorporate the right to privacy in effective public health measures.

2. The question posed in the report of the Special Rapporteur to the General Assembly in 2020 (A/75/147) as to whether, and to what extent, pandemic infringements upon the right to privacy are lawful, proportionate and necessary, was designed to clarify the best approach for the current and future pandemics. The question remains unanswered. There is a dearth of accurate, comparative data, and States' ill-preparedness for the pandemic and accountability shortfalls, combined with their political contexts, have contributed to this opacity.

3. Regardless, the aim of the present report is to shed further light on how pandemics can be managed with respect to the right to privacy. It is largely based on the public consultation on COVID-19 co-convened by the Special Rapporteur with the Global Privacy Assembly and the Organisation for Economic Co-operation and Development, held from 21 to 23 June 2021,[1] and other research.

II. Privacy and personality and coronavirus disease

4. Many measures taken by States to control the spread of COVID-19 have negatively impacted the enjoyment of the right to privacy and other human rights. Negative impacts have been exacerbated by existing structural inequality, social exclusion and deprivation. This public health crisis has exposed the interdependencies between States and the corporate sector, as well as the interrelationships between gender, race, ethnicity and socioeconomic status and health outcomes. Measures to check the spread of the virus have involved restrictions on human rights affecting citizens generally, but with disproportionate impact upon sections of societies.[2]

5. The Special Rapporteur has promoted the wider understanding of privacy beyond informational privacy[3] and surveillance, emphasizing the positive, facilitative aspect of the right to privacy concerning the innate dignity of the person, the contribution of privacy to the enjoyment of other human rights, and its significance for the development of the personality of any given individual. This is consistent with an approach whereby privacy is considered not as a human right in a vacuum but rather in the context of its links to other rights, especially those which it facilitates or otherwise enables. Thus, privacy is an essential prerequisite to the right to unhindered development of personality explicitly recognized in article 22 of the Universal Declaration of Human Rights of 1948: "Everyone … is entitled to realization … of the … rights indispensable for … dignity and the free development of … personality." Article 29 of the Declaration also protects the right to develop one's personality: "everyone has duties to the community in which alone the free and full development of … personality is possible." One of the most significant examples of linking of the right to privacy and the right to personality in United Nations discourse since the publication of the Declaration may be found in Human Rights Council resolution 34/7 on the right to privacy in the digital age, in which the Council recognizes "that the right to privacy can enable the enjoyment of other rights and the free development of

[1] Special recognition is due to Prof. Elizabeth M. Coombs, Mr. Ketan Modh and Mr. Halefom Abraha for their assistance in compiling and editing the present report.

[2] "Epidemics have gendered effects", Clare Wenham, Associate Professor of Global Health Policy, London School of Economics and Political Science, cited by Martha Henriques, 13 April 2020. See www.bbc.com/future/article/20200409-why-covid-19-is-different-for-men-and-women.

[3] Sometimes erroneously used interchangeably with its subset "data privacy".

an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association". Comprehensive human rights metrics for the success of anti-COVID measures must therefore take into account a number of rights which are closely interwoven in a continuously increasing complexity thanks to a number of technologies, in particular Internet access, photography and telephony, which converge most significantly in smartphone use.

6. As clearly emphasized in the text, the Special Rapporteur's first report on the COVID-19 pandemic[4] was necessarily, like the present document, an interim report based only on the evidence available after only four months of experience of the pandemic. Its main thrust was thus to outline the relevant authorities and legal basis for public health measures and the right to privacy. That report did not cover the effects of pandemic measures upon all aspects of privacy or the differential impact of COVID measures upon different groups within society, most particularly those in vulnerable and marginalized situations. These significant issues reflect the quality of a society and its governing institutions. The successful incorporation, or otherwise, of all human rights in pandemic management is a measure of this quality.

7. The report of the Special Rapporteur to the Human Rights Council in 2021 (A/HRC/46/37) highlighted the effect of COVID-19 effect upon the privacy of children. School closures affected approximately 90 per cent of the global student population. Downloads of education applications in 2020 increased 90 per cent compared with the weekly average in late 2019.

8. The shift to online education amplified existing power imbalances between educational technology companies and children, and between Governments and children and parents. Several Governments waived child data privacy laws. In other places, for example some Australian states, no protection exists for children's right to privacy in government schools, although non-State actors routinely control children's digital educational records. These digital records include thinking characteristics, predicted learning trajectories, engagement scores, response times, pages read and videos viewed.

9. One cannot divorce pandemic management from education, and likewise one cannot ignore the links between education, privacy and pandemic management. When the pandemic forces more and more teaching to go online, the privacy impact may be hidden but may be significant nevertheless. This is especially true since in most countries education is compulsory from an early age and most children and parents cannot challenge the privacy arrangements of educational technology companies or refuse to provide data despite legitimate concerns. In late 2020, for example, an analysis of 496 educational technology applications in 22 countries found that many were collecting device identifiers, 27 applications were taking location data, and 79 out of 123 manually tested applications were sharing user data with third parties, such as advertising partners. Data security risks are indicated. Microsoft, for example, reported 5.7 million malware incidents affecting users of its education software from 24 August to 24 September 2020.[5]

[4] A/75/147.

[5] See Quentin Palfrey and others, "Privacy considerations as schools and parents expand utilization of Ed Tech apps during the COVID-19 pandemic", International Digital Accountability Council, 1 September 2020. Available at https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf.

10. Seemingly simple measures to contain the coronavirus have had unintended consequences, some of which are relevant to the protection of privacy of the individual. Designating different days when men and women can leave their homes for essential activities such as obtaining food and accessing health services,[6] has adversely affected transgender communities.[7] Restricting the free movement of people according to gender increases the risk to lesbian, gay, bisexual, transgender and intersex (LGBTQI) people of being "outed" and abused during security force and police identity checks. Since the onset of the pandemic, often life-saving gender-affirming medical care also has been deemed "non-essential" in many States.

11. Physical integrity and autonomy are linked to privacy. Domestic spaces are by their very nature more private but confinement to a domestic space during a pandemic may be problematic for other reasons. A rise in gender-based domestic violence by intimate partners and family members has been reported during lockdowns.[8] For some children, lockdown measures have increased their risk of being subjected to physical or psychological violence at home and limited the possibility of contact with adults to whom such violence might be reported.[9]

12. Human rights assessments prior to and during the pandemic would have mitigated the risks identified above and are therefore an essential component of policy direction for the future.

III. Privacy, other human rights and coronavirus disease

13. The pandemic has raised questions about rights and their place in a democracy. In 10 of the 13 countries surveyed in both 2020 and 2021, feelings of social division have increased significantly since the start of the pandemic.[10] While vaccine passports for example, are meant to improve access to rights and ease travel restrictions, they exclude those who do not have access to vaccines, cannot be vaccinated for health reasons or choose not to be vaccinated. The proportion of the world population that cumulatively falls into these categories is currently very large.[11]

14. People around the world have ceded aspects of their privacy and freedoms to their Governments in order to stem the coronavirus. Measures taken by countries have affected freedom of expression (57 countries); freedom of assembly (147 countries); and the right to privacy (60 countries).[12] Assessment of the proportionality of and necessity for these incursions is overdue.

15. As COVID-19 surveillance measures remain in place and are even extended, Governments will have greater access to personal data linked to location, medical

[6] For example, Panama and Peru, among others. See www.reuters.com/article/us-health-cronavirus-peru-idUSKBN21K39N, April 2020.

[7] Gender identity falls under privacy. See Human Rights Committee, *G. v. Australia*, (CCPR/C/119/D/2172/2012), para. 7.2.

[8] See COVID-19 and increase in gender-based violence and discrimination against women, Joint call by the EDVAW Platform of independent United Nations and regional expert mechanisms on violence against women and women's rights on combating the pandemic of gender-based violence against women during the COVID-19 crisis, 20 July 2020. Available at https://rm.coe.int/edvaw-statement-covid-19-and-vaw-final/16809efd2c.

[9] A/HRC/46/19, para. 17.

[10] See Pew Research Center survey conducted from 1 February to 26 May 2021, among 18,850 adults in 17 advanced economies. Available at www.pewresearch.org/fact-tank/2021/06/24/eu-seen-favorably-across-17-advanced-economies-but-views-vary-on-its-coronavirus-response/.

[11] See OECD, "Access to COVID-19 vaccines: global approaches in a global crisis", OECD Policy Responses to Coronavirus (COVID-19) (18 March 2021).

[12] See International Center for Not-for-Profit Law, COVID-19 Civic Freedom Tracker. Available at www.icnl.org/covid19tracker/?issue=5.

history and other sensitive information about people's lives and finances. It appears that some States are unlikely to relinquish their new powers and mass surveillance tools once the health crisis recedes. In China, an app developed to track the coronavirus is being made permanent in some cities. Even more worryingly, "a new system uses software to dictate quarantines and appears to send personal data to police, in a troubling precedent for automated social control".[13] These risks are said to be most pronounced in Asia,[14] but in all countries, including democracies, authorities can exploit data for political ends with accompanying losses of human rights. Emergency pandemic measures pose risks requiring emergency-quality protections.[15]

IV. Data protection, technology, surveillance and coronavirus disease

16. COVID-19-related data is health data, which is the first category of personal data to qualify for special levels of protection under international, regional and national laws. An overall framework for the protection of health data has already been the subject of comprehensive recommendations[16] and a detailed explanatory memorandum[17] submitted by the Special Rapporteur to the General Assembly in October 2019 but it is estimated that approximately 75 per cent of United Nations Member States fall significantly short of the standards set out in those documents. All available evidence suggests that these shortcomings were further exacerbated by the COVID-19 pandemic.

17. Effective responses to health crises require the collection and management of sensitive data and necessitate strong privacy safeguards. In many cases, however, systems to limit data processing to what is strictly required for specific health-related purposes were not, and are not, in place.

18. Transparency guarantees regarding data processing and safeguards for addressing data breaches are absent in many countries. In others, existing data protection requirements were not followed, for example, the European Union Digital COVID Certificate proposed by the European Commission on 17 March 2021, a year after the declaration of the pandemic in March 2020, did not undergo an impact assessment: "in view of the urgency, the Commission did not carry out an impact assessment."[18]

19. Such shortcomings undermine public health efforts and public confidence in them. Sixty per cent of Americans, for example, believe that if the Government tracked people's locations through their mobile phones it would not make much difference to containing COVID-19.[19]

20. Data is integral to many pandemic measures, and time has seen COVID-19 also become a "data crisis". Both Governments and technology companies are processing personal and health-related data raising concerns about the necessity and proportionality of data collected, the collection methods, security and secondary uses

[13] Paul Mozur, Raymond Zhong and Aaron Krolik, "In Coronavirus fight, China gives citizens a color code, with red flags", *The New York Times*, 1 March 2020, updated 28 January 2021.

[14] See Sofia Nazalya, "Human Rights Outlook 2020", 30 September 2020.

[15] See Graham Greenleaf, "COVID-19: the available evidence … and a little bit of hindsight", 23 June 2021.

[16] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.Pdf.

[17] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

[18] See Explanatory Memorandum to European Union Commission's proposal, sect. 3. Available at eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130.

[19] See Pew Research Center survey conducted in April 2020 Available at www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/.

of this data.[20] A particular concern for LGBTQI people is the non-consensual sharing of health data.[21] Almost half (48 per cent) of Australians are now more concerned about the protection of their location information as a result of COVID-19, and three quarters (75 per cent) believe that COVID-19 does not excuse business or government from meeting their usual obligations under privacy laws.[22]

Technology

21. The technology used to manage the pandemic falls into four broad groups:

(a) Contact-tracing and social-distancing tools relying on Bluetooth proximity tracking;

(b) Quick Response (QR) codes or bar codes used to check in to venues;

(c) Accessing geolocation data through the use of either cell tower history or the Global Positioning System (GPS) to find where people must be alerted because of possible proximity to people testing positive for COVID-19;

(d) Apps to register for vaccinations or download vaccine certificates.

22. There is a lack of data showing the accuracy of some technologies. Indications suggest that technologies in use are unreliable. For example, in Israel, people have successfully contested the quarantine measures applied to them through the use of cell tower triangulation. Of 20,000 people who appealed their isolation orders, 54 per cent (approximately 12,000) were successful.[23] In the United States of America, the American Civil Liberties Union reported that the cell tower data is imprecise.[24]

23. Bluetooth proximity tracking has also been found to lack reliability. In a study of German, Italian and Swiss implementations of Bluetooth proximity tracking on European light trams, detection reliability was found to be akin to triggering notifications by random selection.[25] Reliability involves signal strength, which is affected by: differences between different models/makes of handset; fluctuations in the relative orientation of handsets; absorption by human bodies or containers; and radio wave reflection from walls, floors and furniture.

Pandemic surveillance enabled by data

24. “Surveillance” is a term of art used for epidemiological study and containment of disease. It is also used to refer to security activities linked, for example, to intelligence gathering and law enforcement purposes. Both uses, i.e., medical and security, must be necessary and proportionate.

25. The need to protect citizens’ health saw countries use surveillance to track the spread of infection by:

[20] Ibid.

[21] A/HRC/40/63 2019, para. 84.

[22] Office of the Australian Information Commissioner, 2020.

[23] “Over 12,000 mistakenly quarantined by phone tracking, Health Ministry admits”, *The Times of Israel*, 14 July 2020.

[24] See Jay Stanley and Jennifer Stisa Granick, “The limits of location tracking in an epidemic” (8 April 2020).

[25] See Douglas J. Leith and Stephen Farrell, “Measurement-Based Evaluation of Google/Apple Exposure Notification application programme interface for Proximity Detection in a Light-Rail Tram” (2020) PLOS One, vol. 15, e0239943.

(a) Manual contact tracing, as in Malta;[26]

(b) The use of Bluetooth, GPS, cell tower tracking and bar/QR codes in mobile phones and wearable technology in systems specifically designed for uses in epidemics, as, for example, in the Republic of Korea;

(c) The use of cell tower and other data triangulation sources originally devised as covert counter-terrorist measures but converted to pandemic use, as, for example, in Israel;

(d) Mandatory check-ins with bar codes and QR codes,[27] as in Australia;

(e) Vaccine passports, for instance, the European Union Digital COVID Certificate Regulation, in application since 1 July 2021.[28]

26. The collection and treatment of data from these sources has varied around the world, in terms of the type collected, where it is stored, who has access to it and the autonomy of individuals whose data is collected. Much of the data has been a product of technological responses as well as an input to them. Technological structure is important for the options available to citizens for managing aspects of their right to privacy.

27. Contact tracing apps follow either a centralized or decentralized data approach, whether for contact tracing or vaccine registration. Centralized and decentralized approaches are primarily distinguished by the storage location of the data and how that data is processed. Under the centralized approach, regardless of where the user data is generated, it is stored and processed on a central server operated by public health authorities or on servers of a private company chosen by the Government.

28. In the case of contact tracing apps, the servers calculate updated risk scores for all relevant users and decide which affected users to contact. In vaccine registration, the servers store data on scheduled vaccination periods, vaccination types and status of each individual for administrative purposes.

29. For the authorities, centralized systems allow data collected to be analysed to provide insights into the spread of the pandemic, the most severely affected areas and vaccine coverage, among other uses. This assists the allocation of resources based on established priorities.

30. Australia has two centralized examples: a Bluetooth proximity app (COVIDSafe) and a QR code tracking program for event check-ins. The COVIDSafe app was implemented through the promulgation of specific legislation with privacy safeguards. The QR code tracking programme however, has not been backed by special legislation but depends on previous health regulations and the existing Privacy Act 1988. This deficit is problematic as Australia does not have constitutional safeguards for the right to privacy.

31. The Republic of Korea established a centralized approach through the use of medical facility records, GPS data, card transactions and closed-circuit television,[29] informed by the country's earlier experience with the Middle East respiratory

[26] Jessica Arena, "What is contact tracing and how is Malta doing it?" *Times of Malta*, 23 March 2020.

[27] See for example, Government of South Australia, "COVID SAfe Check-In" (available at www.covid-19.sa.gov.au/business-and-events/covid-safe-check-in) and New South Wales Government, "Setting up electronic check-in and QR codes" (available at www.nsw.gov.au/covid-19/covid-safe/customer-record-keeping/setting-up-electronic-check-and-qr-codes).

[28] See https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en.

[29] See "Contact transmission of COVID-19 in South Korea: novel investigation techniques for tracing contacts" *Osong Public Health and Research Perspectives*, vol. 11, No. 1 (2020), pp. 60–63.

syndrome (MERS) outbreak in 2015. The approach identified routes taken by patients, the risk of exposure for others in their vicinity, the classification of contacts into close and casual and the management of these contacts through quarantine measures.

32. Argentina also implemented a centralized database for the collection of data from the Cuidar app, created through an administrative decision on 23 March 2020.[30] While voluntary for Argentinian residents, it was mandatory for travellers from abroad, with the Bluetooth data accessible by national and provincial governments.

33. Centralized architecture including those in Australia, Israel and the Republic of Korea, raises concerns about the protection and secure storage of sensitive information, including health data, as well as the significant likelihood of centralized databases being re-used by Governments and corporations for other purposes, including political and commercial surveillance.

34. Citizens are distrustful of Governments creating large-scale databases on them. The majority of Australians (60 per cent) for example, agree that some concessions must be made to privacy protections to combat COVID-19 for the greater good as long as this is temporary. However, over half (54 per cent) are now more concerned about the protection of their personal information as a result of COVID-19 management, including 26 per cent who are much more concerned.[31]

35. Decentralized apps provide users with more control over their information. It is kept on their phones, not on a central database accessible by Government or other entities. Examples of a widely adopted decentralized approach include the Google-Apple Exposure Notification System application programming interface, whereby warnings are not processed through a central database but triggered automatically and locally on users' phones.

36. Countries have used a mix of centralized and decentralized measures. Singapore issued wearable tracking devices with Bluetooth to record all interactions with nearby tracking devices, saving this data for 25 days before deletion.[32] This approach led to the development of mobile phone apps for contact tracing, enforcing quarantine measures, monitoring symptoms and providing information on the pandemic, with 46 apps identified as early as August 2020.[33]

37. Intersecting these technical architecture matters is the matter of whether the adopted technologies are mandatory or voluntary. An app can be considered voluntary if a user has the ability to opt out by:

(a) Not installing the app at all;

(b) Turning off the Bluetooth/GPS functionality;

(c) Using the app but refusing to report a positive diagnosis.

38. Although the initial response to voluntary contact tracing apps in Israel and Australia was positive, ultimately a small percentage of the population used them. In Australia, the *Privacy Amendment (Public Health Contact Information) Act 2020*

[30] Available (in Spanish) at: www.boletinoficial.gob.ar/detalleAviso/primera/227116/20200324.

[31] See 2020 Australian Community Attitudes to Privacy Survey. Available at www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/.

[32] See "TraceTogether, safer together". Available at www.tracetogether.gov.sg/.

[33] See Hanson John Leon Singh, Danielle Couch and Kevin Yap, "Mobile health apps that help with COVID-19 management: scoping review", *JMIR Nursing*, vol. 3, No. 1 (2020), e20596.

("COVIDSafe Act") made mandating the use of the COVIDSafe app an offence[34] and initial public assessment was positive with support shown by 70 per cent of those surveyed, but the app is now "all but abandoned".[35] Australian state governments appear more reliant on compulsory check-ins to venues using QR codes. The Republic of Korea exemplifies a national policy initiative that used mandatory location tracking from its conception, with some assigning the successful curbing of the pandemic to the compulsory nature of its policy.[36]

39. Consent and the ability to withdraw it are integral to the right to privacy. This ability is impossible if contact tracing apps are mandatory. Compulsory measures also raise risks of Governments and corporations misusing data collected for combating the pandemic through "surveillance creep" or the repurposing of data without the data providers having any ability to remove their data from databases.

Crossing the line?

40. Many countries were caught ill-prepared to manage rising infections and deaths. A number felt it imperative to address the risks to the health and lives of their citizens through whatever means available. Whether knowingly or unknowingly, the actions taken by some Governments have "crossed the line" in terms of human rights law and what is appropriate and acceptable in democratic societies.

41. The avenues available for surveillance for "public health reasons" and for intelligence or security purposes have sometimes merged and blurred, losing important separations and distinctions. In contexts of adoption of voluntary options supported by citizens, such conduct by States demonstrates how the right to privacy and citizens' autonomy are circumvented.

Israel

42. To illustrate the problem of attempted circumvention of rights, one observes that the Government of Israel declared a state of emergency on 19 March 2020 via the Public Health Ordinance, 1940.[37] The Ministry of Health adopted an app, "HaMagen", which collected users' movement and location information and stored this on the internal memory of their cellular devices unless users opted to send that data to the Ministry of Health, where the data was accessible to employees, representatives and service providers. Thus, the app was both decentralized and (voluntarily) centralized.

43. Alongside this arrangement, the Government of Israel authorized the Israel Security Agency to request and collect cell tower data from telecommunication service providers without the consent of those being monitored. Telecommunication service providers were compelled to trace the movement of people known to be infected against cell tower records by two back-to-back emergency decrees of mid-March

[34] See section 94H of the *Privacy Amendment (Public Health Contact Information) Act 2020:*

> 94H Requiring the use of COVIDSafe
>
> (1) A person commits an offence if the person requires another person to:
>
> (a) download COVIDSafe to a communication device; or
>
> (b) have COVIDSafe in operation on a communication device; or
>
> (c) consent to uploading COVID app data from a communication device to the National COVIDSafe Data Store.
>
> Penalty: Imprisonment for 5 years or 300 penalty units, or both.

[35] Paul M. Garrett and Simon J. Dennis, "Australia has all but abandoned the COVIDSafe app in favour of QR codes (so make sure you check in)", *The Conversation*, 1 June 2021.

[36] See Kyung Sin Park, "Korea's COVID-19 success and mandatory phone tracking" (opennet, 20 October 2020).

[37] Greenleaf, "COVID-19: the available evidence … and a little bit of hindsight" (see footnote 15).

2020, authorizing police to request such data for locating patients, running random checks on those quarantined, and retro-tracing their movements for up to 14 days.[38] The surveillance method used was invalidated by the Supreme Court of Israel in April 2020, compelling the Government to pass a new law to provide the correct legal basis for authorization of the Agency to continue tracing under the Israel Security Agency law. This was followed in July 2020 by the temporary Israel Security Agency authorization law.

44. In early 2021, the temporary amendment of the Public Health Ordinance, 1940 authorized transfer of personal information of unvaccinated individuals to municipalities and education and welfare officials. In early March 2021, the country's Supreme Court prohibited the use of authorization law for mass surveillance and followed this by suspending the application of the amendment.

45. Additionally, it has been reported that vaccine data has been used for: large population research without consent; public disclosure of infection paths; the use of drones for monitoring home quarantine; the use of genetic data companies for COVID-19 testing and the airing of a draft bill for the transfer of epidemiological information to police.[39]

46. The decentralized HaMagen app released by the Ministry of Health was initially positively regarded and identified 30 per cent of initial cases but usage dropped drastically owing to a loss of public trust in the privacy safeguards for the app.[40] The Agency's contact tracing measure would appear to have had limited effectiveness owing to:

(a) The lack of clear data about the benefits of the Agency's program, in absolute and comparative terms;

(b) The tendency of the technology to provide false positives.

47. The system used in Israel is modelled on and uses counter-terrorism technologies. It has been reported that, since mid-March 2020, the Israel 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. The information comes from the communications metadata base of the Agency. Since March, the Government of Israel has tried to strengthen the level of parliamentary scrutiny of its intelligence operations. Unlike France, the Netherlands and the United Kingdom of Great Britain and Northern Ireland, Israel does not possess an independent statutory "expert body" capable of acting as an independent oversight authority to complement the work of the parliamentary committee, so the concern about the ability to carry out detailed and effective scrutiny of such activities by an intelligence service remains significant. Approximately a year after it deployed such privacy-infringing technologies for pandemic use, the crossing of the line by Israel was terminally condemned by the Supreme Court on 1 March 2021, when it banned the Government from the sweeping use of mobile phone tracking of coronavirus carriers, calling the measure a grave infraction of civil liberties.[41] The Special Rapporteur notes reports that these actions, in the case of Israel, have also stifled the

[38] See David M. Halbfinger, Isabel Kershner and Ronen Bergman, "To track Coronavirus, Israel moves to tap secret trove of cellphone data", *The New York Times*, 16 March 2020.

[39] Prof. Yuval Shany, Israel's response to the COVID-19 pandemic: Right to Privacy Aspects, Federmann Cyber Security Research Centre, Hebrew University of Jerusalem; "COVID-19: the available evidence … and a little bit of hindsight" (see footnote 15).

[40] For example, see Mitnick J, "How Israel's COVID contact tracing app rollout went wildly astray" (CIO, 7 November 2020).

[41] See Maayan Lubell, *Israeli Supreme Court bans unlimited COVID-19 mobile phone tracking*. Available at www.reuters.com/article/us-health-coronavirus-israel-surveillanc-idUSKCN2AT279.

development of privacy-friendly apps and epidemiological investigations, and finds that using counter-terrorism powers in a purely health-care setting is contrary to international human rights law and establishes a dangerous precedent.

Republic of Korea

48. Other Governments, such as that of the Republic of Korea, also compelled telecommunication service providers to trace the movement of those known to be infected.[42] The surveillance applied incorporated the use of a smartphone application with a bringing together of 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:

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

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

(c) Details captured by the extensive network of surveillance cameras.

49. It should first be stated that, in most instances identified, the privacy-intrusive measures concerning the COVID-19 pandemic taken within the Republic of Korea had a legal basis. They were provided for by law. The outstanding questions therefore, as ever, remain: were/are these measures necessary and proportionate in a democratic society?

50. In order to answer this question accurately, it is important to examine in detail what actually happened in the Republic of Korea. The technologies employed certainly seem to have been successful in drastically reducing the time taken to identify the locus of the infection and how it was spread:

51. As COVID-19 began to spread, the Government of the Republic of Korea transformed the "Smart City" data platform that it was developing into a public health tracking tool. The Korea Disease Control and Prevention Agency developed the Epidemic Investigation Support System, a platform that enables public health authorities to rapidly collect and analyse data to track confirmed COVID-19 cases. The system began operating on 26 March 2020, just two months after the country's first confirmed COVID-19 case. Using the system, once the Agency confirms a COVID-19 case, authorized investigators request each patient's location data that is entered into the system by respective entities pursuant to the country's Infectious Disease Control and Prevention Act. The system then performs real-time tracking analysis, which, complemented by traditional interviews by human contact tracers, enables both quick contact tracing and the identification of pandemic hotspots. The system has allowed the tracking and investigation of confirmed COVID-19 cases in less than 10 minutes, rather than a day or more, before the system. Data privacy and security are ensured by making sure that only Agency investigators with the necessary legal authority can access the system and by logging every system access for security incidents. To minimize the collection of personal information, the maximum data collection period for each case is set at 14 days, the incubation period of the disease. In addition, the system is temporary: at the end of the COVID-19 pandemic, all the personal information will be destroyed.[43]

[42] See Park, "Korea's COVID-19 success and mandatory phone tracking" (see footnote 36).

[43] See Jiyeon Kim and Neil Richards "South Korea's COVID success stems from an earlier infectious disease failure", 29 January 2021. Available at https://slate.com/technology/2021/01/south-korea-mers-covid-united-states-democracy.html.

52. The Epidemiological Investigation Support System described above is the first of several technology-related measures taken by the Government. Second, the Republic of Korea has been using a smartphone app to monitor compliance by those under isolation or quarantine – those confirmed to have COVID-19, those in close contact with a confirmed case and international travellers. Throughout the pandemic, the Republic of Korea has not closed its borders to any international travellers entering the country. Instead, it has implemented special entry procedures mandating a 14-day self-quarantine and free COVID-19 testing to prevent spread. The Self-Quarantine Safety Protection App is a two-way app that enables the quarantined person to report any symptoms and the designated case officer to monitor the individual's quarantine compliance via GPS-based location data with consent. While quarantine compliance monitoring via the app is strongly recommended, it is not mandatory. Those without smartphones or those who wish to opt out can be monitored via the traditional method of phone calls by a case officer. Nonetheless, the adoption rate of the app was at 91.8 per cent as at 1 September, and both citizens of the Republic of Korea and travellers are reassured by knowing that those at risk of spreading COVID-19 are compliant with self-quarantine measures.[44]

53. The following summary explains some of the reasons why the Special Rapporteur finds that a significant amount of personal data collection in the name of combating the COVID-19 pandemic was, for certain periods of time, especially during the period from January to June 2020, neither necessary nor proportionate:

> Disclosed contact trace data (e.g., "where, when and for how long") help people to self-identify potential close contacts with people confirmed to be infected. However, location trace disclosure may pose privacy risks because a person's significant places and routine behaviours can be inferred. Privacy risks are largely dependent on a person's mobility patterns, which are affected by several regional and policy factors (e.g., residence type, nearby amenities, and social distancing orders). In addition, the results showed that disclosed contact trace data in the Republic of Korea often include superfluous information, such as detailed demographic information (e.g., age, gender, nationality), social relationships (e.g., parents' house) and workplace information (e.g., company name). Disclosing such personal data of already identified persons may not be useful for contact tracing, whose goal is to locate unidentified persons who may be in close contact with confirmed people. In other words, for contact tracing purposes, it would be less useful to disclose the personal profile of the confirmed person and their social relationships, such as family or acquaintances. The detailed location of the workplace could be omitted because, in most cases, it is easy to reach employees through internal communication networks; an exceptional case would be when there is a concern of potential group infection with secondary contagions. Likewise, it is not necessary to reveal detailed travel information of overseas entrants (which were not reported in the main results), such as the arrival flight number and purpose/duration of foreign travels.[45]

54. While condemning the foregoing prima facie unnecessary and disproportionate collection of personal data, the Special Rapporteur also draws attention to ongoing and consistent attempts by the Government and institutions of the Republic of Korea to increase privacy protections despite COVID-19 measures, for example:

[44] Ibid.

[45] See Gyuwon Jung and others, "Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea", *Frontiers in Public Health*, 18 June 2020. Available at www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/ and www.frontiersin.org/articles/10.3389/fpubh.2020.00305/full.

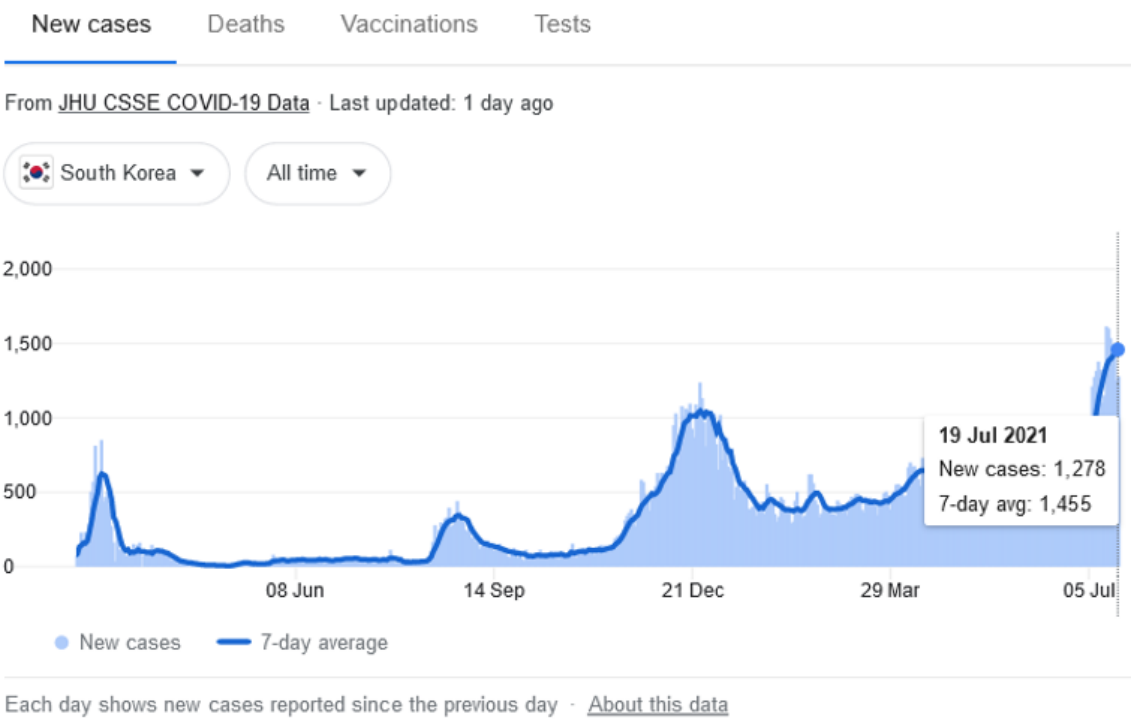
(a) In June and October 2020, the Centers for Disease Control and Prevention issued guidance not to publish patient age, sex, nationality, workplace, travel history or home residency location, although some local governments still disclose some individual travel histories, despite being directed against doing so. Concerns relating to the collection and processing of sensitive personal information, which can reveal intimate information such as a person's sexual orientation and private relations, remained;

(b) In March 2021, the Government of the Republic of Korea asked the public to use their encrypted personal numbers, instead of phone numbers, to protect privacy when they have to write down entry logs at restaurants and cafés, etc., as part of measures to prevent the spread of COVID-19. During February 2021, the Government had rolled out a new privacy protection measure allowing people to use encrypted private numbers for visits to such places: an encrypted number consists of a combination of four numbers and two letters, and it cannot be used for phone calls or text messaging. It can be converted by authorities only when there is an urgent need to contact the holder of the number for virus-related reasons.

55. The Special Rapporteur concludes that, in its attempts to combat COVID-19, the Government of the Republic of Korea took a number of measures that infringed the right to privacy and which, in some cases, were neither necessary nor proportionate. However, in most, if not all of such instances, the Government realized that it had made a mistake and sought to rectify errors through corrective measures (see the examples above).

56. The figure illustrates the pattern of the three waves of COVID-19 during the pandemic in the Republic of Korea from March 2020 to 19 July 2021.

Statistics



Source: Johns Hopkins University.

57. The figure shows that, although the level of infection dipped significantly after the third wave in January 2021, by March and April 2021, it was at the same level as its previous highest peak during the first wave, in March 2020, that is, approximately 530 new cases a day. By 19 July 2021 it had however reached its highest level ever at some 1,300 new cases of infection per day. The precise reasons for this level of infection, despite all of the privacy-intrusive safeguards in place, were not clear at the time of the submission of the present report (20 July 2021). Conclusions at this stage can be only preliminary, since more data is required across a longer timespan for definitive findings to be established. The final verdict is therefore still pending as to whether any or all privacy-intrusive measures regarding the COVID-19 pandemic taken by the Republic of Korea were necessary and proportionate. This makes it difficult to identify which good practices, if any, may be found in the approach of the Government to privacy in the context of the pandemic, except those linked to a reduction in personal data collected, introduced as a remedial measure throughout 2020 and 2021.

58. In Nigeria, nationwide lockdown measures saw deadly repression and violation of human rights where infringements on privacy were probably among the less lethal compared with other severely negative impacts. In addition to restrictions on freedom of movement, it was reported that Nigerian security forces had made unlawful arrests and detentions and extorted and seized and confiscated property.[46]

59. Singapore also provides an example of a line which was crossed and needlessly so, illustrating the problem of function creep quite spectacularly. “Public support took a hit after authorities disclosed in January (2021) that police had used the app’s data in a murder investigation – only months after the minister in charge vowed it would only be used for COVID containment. The Government issued a rare apology. But rather than back down, it plans to formalize the ability of police to access such data in specific cases, introducing the proposed legislation in parliament.”[47] Under the new amendments to the *COVID-19 (Temporary Measures) Act 2020*, passed in the Singapore Parliament in February 2021, personal data collected by digital pandemic contact-tracing programmes can be used only to contact trace, unless it is required by law enforcement for investigations into “serious offences”.[48]

Who’s in charge here?

60. In April 2020, Google and Apple announced a joint effort to enable the use of Bluetooth technology to help Governments and health agencies reduce the spread of the virus. The solution used application programming interfaces and operating system-level technology with greater user privacy and security through a decentralized model.[49] The Google and Apple Exposure Notification initiative set the agenda on decentralized approaches to technological contact tracing via mobiles, owing to their dominance in the smartphone market. It has been used by countries around the world, including Australia, multiple states in the United States and most member States of the European Union. In June 2020, the Government of the United

[46] See Simisola Akintoye, “Privacy implications of national responses to COVID 19 in Nigeria”; De Montfort University; Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight” (see footnote 15); “Coronavirus: security forces kill more Nigerians than COVID-19”, BBC News, April 2020.

[47] See Jamie Tarabay and Bloomberg, “Countries vowed to restrict use of COVID-19 data. For one Government, the temptation was too great”, *Fortune*, 1 February 2021.

[48] See Kirsten Han, “COVID app triggers overdue debate on privacy in Singapore”, Al-Jazeera, 10 February 2021.

[49] See www.apple.com/mt/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

Kingdom was compelled to make a major U-turn and abandon the mode of functioning of its then-current coronavirus-tracing app, shifting to a model based on technology provided by Apple and Google.

61. In April 2021, an update to the contact tracing app for England and Wales was blocked for breaking the terms of an agreement made with Apple and Google.[50] The agreement that all health authorities had signed in order to use Apple's and Google's privacy-centric contact tracing technology stipulated that location data could not be collected via the software. In the proposed update, however, users were asked to upload logs of venue check-ins (poster barcode scans) if they tested positive for the virus.

62. These incidents throw into stark relief the power of big tech companies. Irrespective of the legalities involved and questions as to which body had the most privacy-preserving stance, a debate needs to be had about the appropriateness of government's reliance on the privacy sector to deliver public health tools to its citizens, and the power of that sector to dictate the terms under which it will deliver such tools. France proved however that it can largely go it alone, and the app that it launched in June 2020 had, by May 2021, been downloaded by more than 25 per cent of the French population.[51]

V. Shortcuts and other pandemic mechanisms

63. Many countries were ill-prepared for introducing public health actions such as social distancing, travel restrictions and mask wearing within a short time frame. Shortcuts were taken in different forms and with different implications.

64. Mechanisms have included, first, declaration of emergencies. To date, 108 countries have made emergency declarations[52] to enable, among other things, mandatory contact tracing initiatives. Emergency declarations were made, for example, by South Africa under its *Disaster Management Act* of 2002.

65. Second: rules have been created to sidestep data protection and security. In Austria, amendments were made to the Health Telematics Act 2012 in March 2020 to allow health professionals to transfer health and genetic data via insecure methods such as fax or email.[53]

66. Third: new legislation was introduced. Denmark passed the Epidemic Act in March 2020, curbing:

(a) The right to assembly by creating curfews, restricting access to areas, and banning assemblies and gatherings to 10 persons from 18 March to 8 June 2020;

(b) The right to personal liberty by compelling hospitalization, isolation and vaccination, and detaining individuals without confirmed infection;

(c) The right to respect for privacy by implementing contact tracing apps with obligatory requirements upon people, businesses and public authorities to provide COVID-19 related data, and by data-driven solutions to assess movement patterns, including of individuals.

[50] See "Apple and Google block NHS Covid app update over privacy breaches", *The Guardian*, 20 April 2021).

[51] See Reuters, "French COVID tracing app downloaded by 25 per cent of the population – minister", 23 May 2021.

[52] As at 14 July 2021, International Center for Not-for-Profit Law, "COVID-19 Civic Freedom Tracker" (see footnote 12).

[53] See amendment: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120.

67. The Epidemic Act was amended in February 2021 to introduce parliamentary processes and control mechanisms for the adoption of: intrusive rules and measures; increased transparency and reduction of arbitrary government power; reduced access to compulsory measures against individuals, for instance, making vaccinations voluntary; and judicial control of compulsory measures leading to custodial punishment.

68. Fourth, in other countries, law enforcement and civil entities became operatives for implementing public health regulations. In April 2021, under the *Public Health Act of Malta*, the Superintendent of Public Health delegated authority to enforce pandemic measures, to:

(a) Police and officers of the Local Enforcement System Agency;

(b) Armed Forces of Malta;

(c) Transport Malta;

(d) Malta Tourism Authority;

(e) Environmental Health Directorate.

69. The officials listed were authorized to enter houses and carry out inspections given "a report or reasonable suspicion that there were a number of people gathering together in breach of the regulations". These measures appeared to be without adequate safeguards while challenging principles of necessity and proportionality. Ordinarily, entry into the domestic residence of a private individual requires a judicial warrant, this example demonstrating the considerable scope of health emergency powers.

70. The need to address the roles and responsibilities of public health and law enforcement is also highlighted by calls from law enforcement in other countries, such as the United Kingdom, for power of entry into homes of suspected lockdown breakers as a "useful tool" to enforce lockdown measures.[54]

VI. Other considerations

71. The COVID-19 pandemic is still unfolding and the debate will change with it. Part of the current debate includes the human rights approach to privacy of the European Union, for example, vis-à-vis the consumer protection approach taken by the United States and, to some extent, Australia. The Federal Trade Commission of the United States recently highlighted privacy enforcement in videoconferencing, educational technology and health technology areas by issuing warning letters and scam alerts on identity theft following the move to digital work and schooling.[55]

72. Previous public health crises have influenced how countries have dealt with the present pandemic. For example, the Republic of Korea used compulsory, centralized contact-tracing mechanisms because of its MERS outbreak in 2015. Prior experience led to the revision of the Infectious Disease Control and Prevention Act to protect sex, age, education and nationality variables from public disclosure, but required compulsory disclosure of infection status.

73. The geographical size of a country has affected the privacy protectiveness of certain measures. Smaller countries have had an advantage in handling aspects of the pandemic: for example, despite the high population density of Singapore, it was able

[54] See "Police Chief calls for power of entry into homes of suspected lockdown breakers", Vikram Dodd, *The Guardian*, 5 January 2021.

[55] See *Federal Trade Commission*, "One year into COVID-19 pandemic, new Federal Trade Commission staff report highlights agency's ongoing efforts to protect consumers" (19 April 2021).

to issue hardware tokens to individuals, complementing the use of the TraceTogether smartphone app for those who could not use smartphone apps.[56] Countries such as India, with both a large land mass and population size, on the other hand, introduced online and smartphone-based registration for vaccines through the CoWIN app (connected to an individual's phone number), which did not accommodate the many without access to smartphones or the Internet. Providing hardware tokens (or alternative or anonymized means of registration) requires the issue of many millions of tokens, but not to do so was discriminatory.

74. While not alone, Africa, Latin America, Australia and India have been reported as regions and countries where constitutional protections and/or robust national data protection laws and oversight mechanisms are absent and where this absence undermined Governments' efforts to secure the necessary trust of citizenry in public health measures.

75. Robust national-level data protection laws and strong, independent data protection authorities, or other oversight bodies in some parts of the world, assist contact tracing and vaccination registration initiatives to commence, with due regard to the necessity of protecting citizens' data and communicating that necessity to the community.

76. Most measures collect a lot of sensitive data and it is difficult to estimate whether this collection is proportionate. Even recognized robust data protection laws, such as the General Data Protection Regulation of the European Union, require greater specification and guidance for public health situations.

77. New systems have been layered on top of existing, already complex information technology infrastructure. Data protection authorities in many countries were unable to conduct an evaluation of the technical aspects of these systems, and the accompanying long and highly technical descriptions, due to time frames, resources or expertise – as noted by the Datenschutzrat (Data Protection Council) of Austria in its evaluation of the regional initiative.[57]

78. In general, the strategies used by countries across the world inevitably led to the suspension of fundamental human rights and freedoms. Emergency measures have facilitated rapid, but not necessarily well-thought-through responses. Smartphone apps or other forms of surveillance should be legally acceptable, technically reliable and socially acceptable and tested via a human right assessment which was largely conspicuous by its absence during the period under review.

79. Public trust affects the effectiveness of anti-pandemic measures. While trust in government plays a role in the success of any government initiative, trust is most needed in extraordinary situations such as the COVID-19 pandemic. This is particularly important for voluntary measures where effectiveness relies on the engagement of citizens.

80. Privacy intrusive measures have seen resistance. In the United States, location tracking tools and centralized systems have met determined opposition; as at July 2021, only two states have introduced vaccine passports and many states have banned them.[58] Citizens are concerned that pandemic measures will not be rescinded. In similar vein, the majority of Australians (60 per cent) agree that some concessions

[56] "Token Go Where". See https://token.gowhere.gov.sg/.

[57] See www.bmj.gv.at/dam/jcr:c4b7569c-46c3-4772-bb07-9085f61412a8/Stellungnahme_des_Datenschutzrates_Epidemiegesetz.pdf.

[58] See Elliott Davis, "Which States Have Banned Vaccine Passports?", *US News*, 1 June 2021.

must be made to privacy protections to combat COVID-19 for the greater good, as long as they are not permanent.[59]

81. Technology plays a critical role for Governments in managing public health issues. Its use, however, may normalize future surveillance after the pandemic. For example, government-mandated contact tracing apps could also be used to access user personal data as a government surveillance tool. The normalization of intrusive technologies paves the way to further privacy invasive measures. Businesses, for example, have expanded their surveillance of workers while ostensibly introducing social distance monitoring apps and tokens.

82. The reluctance or inability of Governments to establish the proportionality and necessity of measures may be related to function creep of the technologies and data collected, and/or that these tools are ineffective.

83. The pandemic has created hitherto unforeseen issues owing to the move towards hybrid working environments, with workers being collectively monitored by employers. The measures implemented by companies to monitor social distancing among employees have affected employee privacy. While many businesses had to suspend their activities, others circumvented this suspension by requiring workers to wear devices providing physical proximity alerts. Many businesses are now interested in monitoring teleworking employees by using software to record keystrokes, screenshots and other computer activity. These technologies risk "surveillance creep", while others are showing "mission creep" by no longer storing recorded data from wearable monitoring devices locally but providing it to a central database for no justifiable reason.

84. The COVID-19 pandemic has revealed limitations in existing data protection laws such to cover these emerging risks to personal data and privacy. The General Data Protection Regulation, otherwise considered to be setting the bar for data protection worldwide, does not provide for the ability to raise collective claims since it deals primarily with individual rights.[60]

VII. Conclusions

85. It is times of emergency that establish the real quality of States, Government and private actors, including individuals.

86. International treaties and most national constitutions allow States to temporarily increase their powers during a period of crisis, such as responding to the COVID-19 pandemic. The pandemic has intertwined health and surveillance and individual impacts. It thus requires management within the parameters established for these domains.

87. From a right to privacy perspective, the pandemic has enabled more intrusion by Governments and corporations into people's lives, infringing their right to privacy. While some infringements can be expected to arise during a pandemic, for public health purposes, it has, to date, proven to be impossible to gauge to what extent these have been necessary and proportional.

88. Unfortunately, many States have framed privacy protection as opposed to necessary measures for saving lives. It is a simplistic view that ignores the importance that people attach to their privacy and to limiting unwarranted incursions by

[59] Office of the Australian Information Commissioner.

[60] See Andrew Pakes, "High Visibility and COVID-19: returning to the post-lockdown workplace" (Ada Lovelace Institute, 19 May 2020).

government and the commercial sector into their lives. The result is resistance to government's pandemic management efforts.

89. The COVID-19 pandemic has seen shortcuts taken around the world in implementing national public health strategies. Some Governments have made use of emergency laws to pass mandatory contact tracing initiatives; others have taken advantage of the lack of robust national-level data protection laws to quickly roll out solutions such as contact tracing and registration of vaccinated individuals without paying heed to the right to privacy, or other human rights. Crisis responses, some of the "knee-jerk" variety, have included the exploitation of emergency laws and weak or non-existent data protection laws. Looming elections appear to have been, and continue to be, important factors for a number of States and Governments.[61]

90. Technological tools have been used by Member States to track infections, enforce quarantine measures, maintain social distancing rules and track the administration of vaccines. These tools have been developed by government agencies and corporate entities.

91. In this context, countries were ill-prepared for the exertion of the independence and power of technology companies, such as the stance of Apple and Google on privacy for contact tracing app users. At the same time, it is important to acknowledge that these two companies appear to have been reasonably privacy-protective in their approach, in some cases possibly more so than some of the States which were keen to use the data they collected.

92. The ongoing pandemic means that the promotion and protection of the right to privacy and related rights requires ongoing monitoring and public reporting by bodies at the international, regional and domestic levels.

93. Centralized approaches, including those in Australia, Israel and the Republic of Korea, present privacy risks, such as the protection and storage of sensitive information, including health data, the significant likelihood of these centralized databases being reused by Governments and corporations, as well as the risk of a high degree of data retention. Decentralized apps provide users with more control over their information since all contact information is kept only on users' phones, and there is no central database accessible by the Government or authorities.

94. The privacy implications of compulsory contact tracing apps are obvious – consent and the ability to withdraw it have been recognized at law as integral parts of the right to privacy in many – although not all – cases. Compulsory measures also raise the risks of Governments and corporations misusing the sensitive data collected for the purpose of combating the pandemic through either "surveillance creep" or the repurposing of data without the users having any ability to have their data removed from databases. Voluntary contact tracing apps have suffered from low uptake, typically due to the lack of public trust in the Government's ability to keep their data safe and protected.

95. There are also multiple implementation issues with the technology, including the lack of data showing the accuracy of some technologies. Most of the measures discussed collect a lot of sensitive data and it is difficult to estimate whether this collection is proportionate. While technology plays a critical role in the pandemic, it may also normalize surveillance in the future. Intensive and omnipresent technological surveillance is not the panacea for pandemic situations such as COVID-19.

96. Other related issues include equality and worker privacy protection. Gaps have been revealed in data protection law, including the General Data Protection

[61] See www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections.

Regulation. Better guidance is required on their interpretation and amendment of their provisions. These laws are generally concerned with individual rights, not collective claims of privacy, which will become important as artificial intelligence comes to the fore and, for example, more workers move to hybrid work environments.

97. There is a pressing need for common privacy data principles that can be applied to all legislation that provides for data collection initiatives in dealing with the pandemic. These principles would set a common, interoperable standard for the current pandemic, but also for future occurrences. Such a set has been proposed by Graham Greenleaf and adapted here to include a privacy by design focus.[62]

98. The best time to prepare for a future pandemic is now.[63] These are lessons not just for COVID-19 but for other notifiable and communicable diseases and possible future pandemics.

VIII. Recommendations

99. These are aimed at ensuring the right of every person to enjoy the right to privacy during the current and future public health crises, without arbitrary interference, as set out in the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (art. 17) and the findings of treaty bodies.

100. The recommendations below are intended to cover both State and non-State actors.

Privacy and personality

101. **States and non-State Parties should implement the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework with the gender guidance thereon (A/HRC/41/43, annex).**

102. **Adopt the recommendations of the Special Rapporteur on the right to privacy for protecting against gender-based privacy infringements (A/HRC/43/52, paras. 33 and 34).**

103. **Encourage partnerships with civil society and industry to co-create strategies and technological responses.**

104. **Involve groups in the community at particular risk in consultations on specific public health measures.**

105. **Reduce pandemic response infringements of privacy based on gender by requiring gender-aware privacy human rights impact assessments before introducing measures, strategies and legislation.**

106. **Regularly evaluate the effectiveness of the measures taken to include those in vulnerable and marginalized situations in response and recovery efforts.**

Children

107. **Develop comprehensive online educational plans of action based on article 29 (1) of the Convention on the Rights of the Child and the Council of Europe guidelines on children's data protection in an education setting.**

[62] See Greenleaf, "COVID-19: the available evidence … and a little bit of hindsight" (see footnote 15).

[63] See "The best time to prevent the next pandemic is now: countries join voices for better emergency preparedness" (WHO, 1 October 2020).

108. **Ensure that appropriate legal frameworks are established and maintained for online education.**

109. **Create public infrastructure for non-commercial educational and social spaces.**

110. **Ensure that children's personal data is processed fairly, accurately and securely, in accordance with a legitimate legal basis, utilizing data protection frameworks representing best practice, such as the General Data Protection Regulation and Convention 108+.**

Informational privacy

111. **Build human rights into the design, development and deployment of technological approaches to the pandemic.**

112. **Legislative protections based on common principles with guidance for specific situations are needed for all types of pandemic health measures. The Special Rapporteur recommends the use of the 11 common principles[64] for centralized and decentralized public health surveillance systems, legislative measures for communicable diseases and their utilization when assessing pandemic prevention policies across the world:**

(a) **Establish "privacy by design" and "by default" from the outset by incorporating an overarching human rights assessment alongside a data protection assessment for public health measures with a special focus on epidemics and pandemics;[65]**

(b) **Privacy should be considered from the very beginning of the response to any epidemic or pandemic. Indeed, it should be a cornerstone of any national strategy on how to deal with an epidemic, well thought out, years in advance as an integral – and well-integrated – part of the overarching human rights assessment mentioned above;**

(c) **Insert clear and detailed controls in the region's or individual country's data privacy law;**

(d) **To provide the necessary clarity and legal foundation more effectively than by delegated acts or regulations, and achieve greater uniformity in the jurisdiction;**

(e) **Guarantee access to sites, events, facilities, education, etc., to avoid discrimination;**

(f) **It is vital to protect vulnerable groups adversely and differentially impacted by pandemic surveillance measures;**

(g) **Minimize and define authorized uses of COVID data to ensure that COVID-19 data is not used for other purposes once collected;**

(h) **Establish "purpose specification" as in many existing data protection laws;**

(i) **Minimize data collection;**

[64] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875920.

[65] See Council of Europe "2020 Digital Solutions to Fight COVID-19 2020", Data Protection Report October 2020. Available at www.coe.int/en/web/data-protection/-/digital-solutions-to-fight-covid-19-council-of-europe-report-on-data-protection-2020.

(j) **To ensure that data collection measures are proportionate, establish a generally accepted risk management approach and assist in limiting the damage caused by data breaches, cyber incidents and function creep;**

(k) **Anti-coercion provisions: the requirement to use or show proof of use should be prevented or strictly defined and contained by legislation. Other demands or requests to see certificates of use should be prevented by defining such behaviour as an offence under the law. Enforcement is needed, as are remedies;**

(l) **Prevent "surveillance creep": avoid following the example set by Singapore, which in 2020 promised "tracing only"; then reneged in 2021, allowing criminal investigations;**

(m) **The voluntary participation required by most pandemic prevention measures needs public trust to work. Future expansion as a surveillance measure to other areas for example, criminal investigations, must be made unlawful for this trust to exist;**

(n) **Continuous deletion programme (if data is collected): the legislation itself should require continuous deletion of any collected data within a short period of time, such as the individual's infectious period or some other evidence/scientifically based time period;**

(o) **"Sunset clause" for whole system and mandatory, independent "audit of closure" of all epidemic data systems must be entrenched in law and strictly enforced: establish a fixed period or independent assessment of necessity to ensure that pandemic surveillance systems are shut down, with a statutory based requirement for independent audit that this has occurred;**

(p) **Supervision and periodic public reporting by independent data protection authority: supervision of these surveillance systems must be external and independent;**

(q) **Transparency: the necessary conditions should be identified in consultation with experts and civil society. It may take the form of releasing any source code used to build surveillance systems (such as contact tracing apps), conducting comprehensive data protection impact assessments and releasing data on the effectiveness of techniques used for pandemic surveillance.**

113. **An ongoing dialogue with the big tech companies should complement formal and informal public debate of the roles and responsibilities of big tech companies in carrying out a privacy-protective role in pandemics.**

Transparency and metrics

114. **Health emergency powers require assessment for their necessity and proportionality. As part of this periodic and regular assessment:**

(a) **The Special Rapporteur on the right to privacy, alone, as well as together with other mandate holders, should revisit the situation regarding notifiable and communicable diseases with a special focus on COVID-19, but not limited to COVID-19, at a minimum every 24 to 36 months in order to identify existing and emerging risks, as well as understand the most effective and privacy-friendly policy initiatives that can be used to prepare for pandemics within a holistic approach to human rights protection;**

(b) **If a State decides that technological surveillance is necessary as a response to the global COVID-19 pandemic, it must prove both the necessity and proportionality of the specific measure and establish a law that explicitly**

provides for such surveillance measures containing mandatory explicit and specific safeguards;

(c) **States and corporations should build human rights into the design, development and deployment of technological approaches to the pandemic, given the enormous implications of digital technologies for a broad range of rights, particularly privacy;**[66]

(d) **States and corporations should adopt user-centric, rights-respecting technological design whereby, for example, in the case of "vaccine passports", travellers can carry their data themselves for presentation upon request;**

(e) **External review of States' pandemic responses is required, and States' pandemic management should be assessed, together with other internal human rights responsibilities in their regular periodic reviews at the United Nations level.**

[66] See A/HRC/46/19.