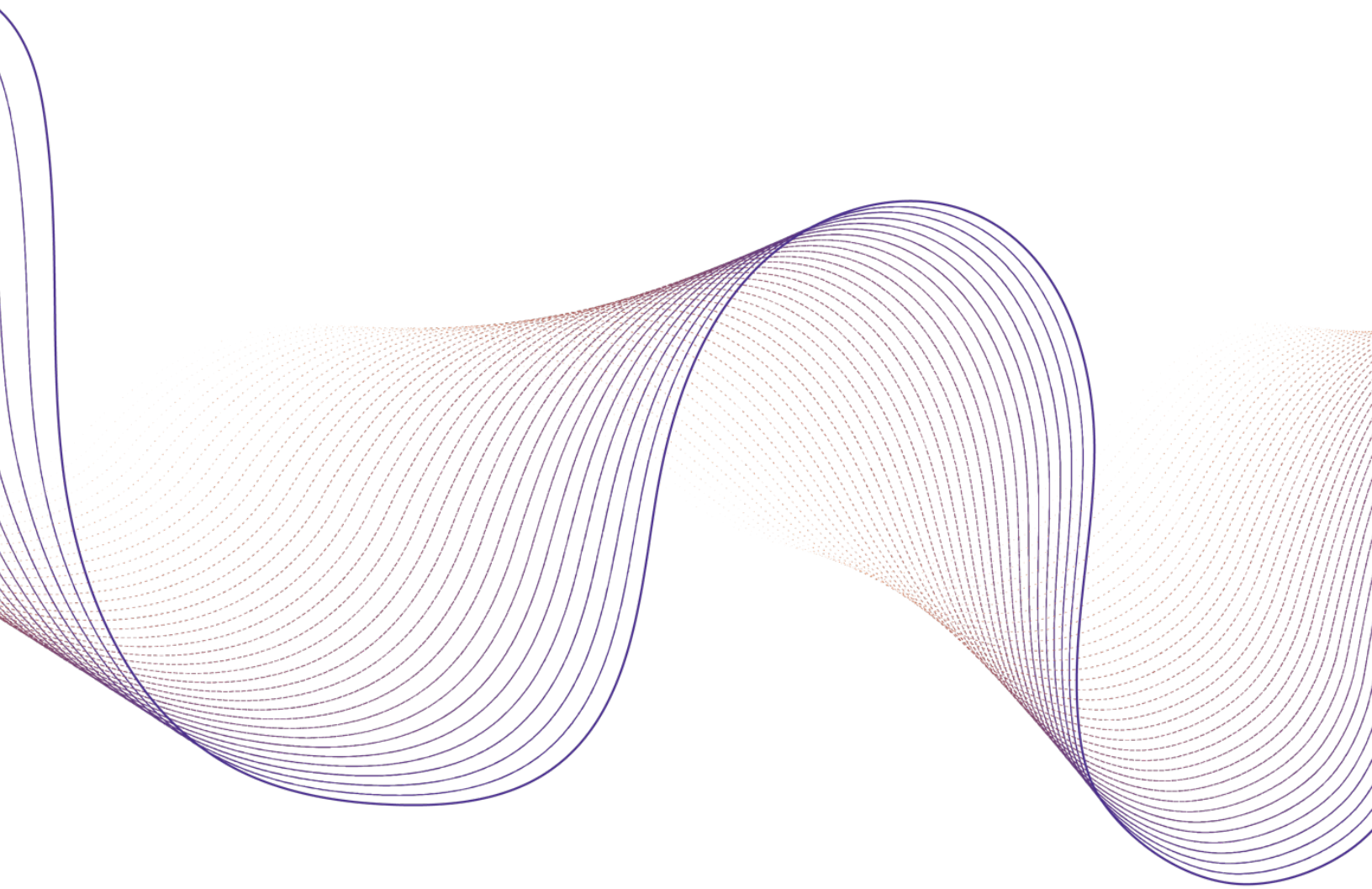
World Justice Project

Privacy, Mass Electronic Surveillance, and the Rule of Law in Times of COVID-19

*Tatsiana Ziniakova**



Introduction

COVID-19 is one of the first pandemics to occur in the digital age. Although the world has already faced SARS, H1N1 influenza, MERS, and Ebola, the global scale of the COVID-19 outbreak remains unprecedented.[1] While the "coronacrisis" re-opened a sorely needed discussion on the possible tech-based responses to global health emergencies,[2] it could also be a perfect storm to undermine key elements of the rule of law. On one hand, new technologies allow states to cooperate closer than ever to curb the global epidemiological threat. On the other, they too easily can be used as tools to threaten fundamental rights, access to justice, and accountable governance.

Technological capabilities of the digital age, used and misused in the COVID-19 pandemic, influence multiple areas of law–from public international law principles of non-intervention and prohibition of the use of force[3] to the human rights to life, health, expression, and non-discrimination.[4] Mindful of the inevitable intersections among these fundamental freedoms, this paper will specifically concentrate on the right to privacy,[5] as affected by surveillance practices.

Tech-based responses to COVID-19 deeply affect the privacy realm. Against the backdrop of a pandemic, states across the globe are resorting to drone surveillance,[6] facial recognition technologies,[7] contact-tracing and quarantine-enforcement apps.[8] The violations of privacy—already manifest pre-COVID—could become routine post-COVID. The emergency thinking that prompted many states to adopt surveillance measures may lead to unpredictable results and further deteriorate privacy in the short and long term.[9]

The purpose of this paper is threefold. First, it summarizes how privacy and surveillance are regulated by international law in the digital age and what the specific privacy regulations applicable to health data are. Second, it seeks to provide an overview of digital surveillance measures applied in times of COVID-19.

---

* Tatsiana Ziniakova is an Engagement Team Intern with the World Justice Project and an Edmund S. Muskie Internship Program grantee. She earned her LL.M. from Wake Forest University, School of Law as a Fulbright scholar and LL.B. from Belarusian State University, Faculty of International Relations.

[1] Gavi: The Vaccine Alliance, How Does COVID-19 Compare to Past Pandemics?, 1 June 2020, https://www.gavi.org/vaccineswork/how-does-covid-19-compare-past-pandemics

[2] Tech-based public health solutions have been considered prior to the COVID-19. See, for instance: World Health Organization, mHealth: New Horizons for Health through Mobile Technologies, 2011, https://www.who.int/goe/publications/goe_mhealth_web.pdf?

[3] See, for instance, Milanovic, Marko and Schmitt, Michael N., Cyber Attacks and Cyber (Mis)information Operations during a Pandemic, Journal of National Security Law & Policy, 27 May 2020. Available at SSRN: https://ssrn.com/abstract=3612019 or http://dx.doi.org/10.2139/ssrn.3612019, pp. 5-12

[4] Ibid., pp. 12-19

[5] Note that the right to privacy is closely connected with freedom of expression. See Part IV, A Interrelations between the rights to privacy to freedom of opinion and expression of Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, A/HRC/23/40, 17 April 2013, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40

[6] Henry Shwan, Drones in Florida Remind Residents to Keep Their Social Distance, Governing, 15 April 2020, https://www.governing.com/now/Drones-in-Florida-Remind-Residents-to-Keep-Their-Social-Distance.html; Matthew Guariglia, Using Drones to Fight COVID-19 is the Slipperiest of All Slopes, Electronic Frontier Foundation, 5 May 2020, https://www.eff.org/deeplinks/2020/05/using-drones-fight-covid-19-slipperiest-all-slopes

[7] Jacob Ward and Chiara Sottile, A facial recognition company wants to help with contact tracing. A senator has questions, NBC News, 30 April 2020, https://www.nbcnews.com/tech/security/facial-recognition-company-wants-help-contact-tracing-senator-has-questions-n1197291; Transnistra News, Moldova: Transnistria uses facial recognition to identify quarantine violators, 28 March 2020, https://novostipmr.com/ru/news/20-03-28/narushiteley-samoizolyacii-vyyavlyayut-s-pomoshchyu-sistemy; Dhaka Tribune, Bangladeshi developers devise a surveillance system to identify people with masks, 7 April 2020, https://www.dhakatribune.com/bangladesh/2020/04/07/bangladeshi-developers-devise-a-surveillance-system-to-identify-people-with-masks

[8] Elliot Alderson blog, Covid19 Tracker Apps, https://fs0c131y.com/covid19-tracker-apps/; Privacy International, Tracking the Global Response to COVID-19, https://privacyinternational.org/examples/tracking-global-response-covid-19; GDPR Hub, Projects using personal data to combat SARS-CoV-2, https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2; MIT Technology Review, Covid Tracing Tracker, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

[9] See Austin, Lisa M. "Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State." Law, Privacy and Surveillance in Canada in the Post-Snowden Era, edited by Michael Geist, University of Ottawa Press, 2015, pp. 103–126. JSTOR, www.jstor.org/stable/j.ctt15nmj3c.8. at p. 105: "This framework of emergencies, with its themes of uncertainty and unenforceability, is both helpful and unhelpful when applied to state surveillance."

Third, it seeks to outline international legal standards against which the lawfulness of COVID-related surveillance measures should be evaluated.

The key finding of the paper is that states resorting to surveillance-based responses to a global health emergency must frame such responses as limitations of or derogations from the right to privacy. Guarantees of international human rights law do not cease to apply in a pandemic and continue to protect individual privacy. To remain compliant with international human rights obligations, states must strictly follow both procedural and substantive requirements for introducing limitations or derogations, including the principles of legality, necessity, and proportionality. Using these well-established frameworks, the new pandemic-related surveillance measures must be assessed against these standards on a case-by-case basis.

1. Privacy in the Digital Age: Development and Evolution

1.1. General regulation

The right to privacy is enshrined in major international and regional human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR),[10] the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR),[11] and the American Convention on Human Rights (ACHR).[12] All of these human rights instruments protect private and family life of individuals, as well as their home and correspondence from unlawful interference.

As with most fundamental human rights, the right to privacy is not absolute. Privacy provisions of human rights treaties both declare the fundamental right to privacy and provide a framework for lawful limitations thereof. Article 17 of the ICCPR states that interferences with the right to privacy must not be "arbitrary or unlawful."[13] Article 11 of the ACHR provides that interferences must not be "arbitrary or abusive."[14] Article 8 of ECHR elaborates the conditions for limitations even more comprehensively, stating that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[15]

In its vast body of surveillance-related jurisprudence, the European Court of Human Rights (ECtHR) provides guidance as to how these limitations on the right to privacy must be interpreted. In Klass and Others v. Germany the ECtHR ruled that the limitation on the right to privacy in the form of telephone-tapping and inspection of mail, was lawful,[16] using the three-part test, derived from Article 8 (2) of the ECHR and consistent with the Human Rights Committee interpretation of "arbitrary or unlawful"

[10] United Nations, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171, Article 17. See also Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, https://www.refworld.org/docid/453883f922.html
[11] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, Article 8
[12] Organization of American States, American Convention on Human Rights, 22 November 1969, Article 11. For more international instruments containing the right to privacy in their provisions see Privacy International, Guide to International Law and Surveillance 2.0, February 2019, https://privacyinternational.org/sites/default/files/201904/Guide to International Law and Surveillance 2.0.pdf, pp. 3-5
[13] United Nations, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171, Article 17 (1)
[14] Organization of American States, American Convention on Human Rights, 22 November 1969, Article 11 (2)
[15] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, Article 8 (2)
[16] Ibid., para. 60, p. 23

interferences with privacy under Article 17 of ICCPR.[17] The test requires answering the following questions:

1. Was there an interference with the right to privacy?

   The applicants are expected to show the disputed measures indeed exist and amount to an interference with privacy.[18]

2. Was the interference conducted in accordance with law?

   This requirement has grown to include two elements. First, the interference with privacy must have a basis in domestic law. Second, the law must be sufficiently "foreseeable," so that individual citizens are able to understand under what circumstances they may be subjected to surveillance, what oversight mechanisms will be in place to protect their rights, and when the collected data will be deleted. Overly vague statutes sanctioning surveillance do not satisfy this criterion.

3. Was the interference necessary in a democratic society to achieve a legitimate aim?

   This requirement, sometimes split in two (necessity in a democratic society and legitimate aim), is meant to assess the proportionality of surveillance ends (e.g., national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedoms of others) and means. Lawful surveillance measures are expected to do only what is "strictly necessary"[19] for the furtherance of the declared legitimate aim.

   In Weber and Saravia v. Germany the ECtHR, despite declaring the case inadmissible,[20] produced a list of minimum safeguards the governments must have in place for surveillance measures to be considered lawful. The list, which came to be called the "Weber Six" in academia,[21] includes the following categories of information that must be available to the potential targets of surveillance: the grounds that may give rise to surveillance; the categories of people who could be subject to surveillance; the limit on the duration of surveillance; the procedure to be followed for examining, using, and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the collected data may or must be erased.[22]

   Although early ECtHR surveillance decisions in Klass and Weber have not fully confronted the vastness of surveillance in the digital realm, they have set a solid framework for analyzing tech-based privacy intrusions. In the aftermath of Snowden revelations of 2013,[23] the digital privacy agenda was mainstreamed within and beyond international human rights frameworks. Parameters around digital intrusions on privacy were issued through United Nations General

[17] Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, https://www.refworld.org/docid/453883f922.html
[18] Although factually intertwined, this requirement is formally separate from showing that the applicants qualify as victims of the alleged violation (whether direct, indirect, or potential). Victim status, along with other conditions, must be proved to show the application's admissibility before the ECtHR, but is distinct from substantive analysis of the alleged violation. See ECtHR Admissibility Guide on all criteria of admissibility: https://www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis/admi_guide
[19] ECtHR, Klass and Others v. Germany, Application no. 5029/71, Judgement of 6 September 1978, para. 43, p. 17
[20] ECtHR, Weber and Saravia v. Germany, Application no. 54934/00, Admissibility Decision of 29 June 2006, para. 78, p. 18.
[21] Lubin, Asaf, "We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance, Chicago Journal of International Law: Vol. 18: No. 2, Article 3, https://chicagounbound.uchicago.edu/cjil/vol18/iss2/3, p. 543
[22] ECtHR, Weber and Saravia v. Germany, Application no. 54934/00, Admissibility Decision of 29 June 2006, para. 95, p. 22
[23] Greenwald, Glenn, NSA collecting phone records of millions of Verizon customers daily, The Guardian, 6 Jun 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Assembly resolutions,[24] decisions of the UN Human Rights Council,[25] and UN independent expert reports.[26] In 2015, the UN Human Rights Council established a new mandate of the Special Rapporteur on the right to privacy[27] to address the dimensions of privacy in the surveillance state.[28] Jurisprudence and observations of judicial[29] and quasi-judicial[30] bodies continued to grow and develop, alongside comprehensive analytics[31] and new international instruments.[32]

1.2. Health data regulation

Although general rules on privacy apply to all aspects of an individual's life, including her medical history, the protection of health-related data is often subject to additional privacy guarantees. A useful example is the EU General Data Protection Regulation (GDPR). Praised for its unmatched privacy safeguards, GDPR affords special protection to health-related data.

---

[24] United Nations General Assembly, Resolution 69/166, The right to privacy in the digital age, A/RES/69/166, 18 December 2014, https://undocs.org/A/RES/69/166; United Nations General Assembly, Resolution 71/199, The right to privacy in the digital age, A/RES/71/199, 19 December 2016, https://undocs.org/A/RES/71/199

[25] Human Rights Council, Resolution 28/ L.27, The right to privacy in the digital age, A/HRC/28/L.27, 24 March 2015, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/061/64/PDF/G1506164.pdf; United Nations General Assembly, Resolution 71/199, The right to privacy in the digital age, A/HRC/71/199, 19 December 2016, https://undocs.org/A/RES/71/199; Human Rights Council, Resolution 34/L.7/Rev.1, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 March 2017, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf

[26] Office of the United High Commissioner for Human Rights, Report on the Right to Privacy in the Digital Age, A/HRC/27/37, 30 June 2014, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; Office of the United High Commissioner for Human Rights, Report on the Right to Privacy in the Digital Age, A/HRC/39/29, 3 August 2018, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf; Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age, A/HRC/29/32, 22 May 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf; Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, on freedom of expression, states and the private sector in the digital age, A/HRC/32/38, 11 May 2016, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf; United Nations General Assembly, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, on Artificial Intelligence technologies and implications for the information environment, A/73/348, 29 August 2018, https://www.un.org/ga/search/view_doc.asp?symbol=A/73/348; Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, on surveillance and human rights, A/HRC/41/35, 28 May 2019; Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, on disease pandemics and the freedom of opinion and expression, A/HRC/44/49, 23 April 2020; United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, on counter terrorism and mass digital surveillance, A/69/397, 23 September 2014, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf; United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, A/HRC/34/61, 21 February 2017, https://undocs.org/A/HRC/34/61

[27] Human Rights Council, Resolution on the right to privacy in the digital age 28/16, A/HRS/RES/28/16, 1 April 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf

[28] All reports of the Special Rapporteur on the Right to Privacy are available at: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx. Kinfe Michael Yilma, The United Nations' Evolving Privacy Discourse and Corporate Human Rights Obligations, 23(4) ASIL Insights, 17 May 2019, https://www.asil.org/insights/volume/23/issue/4/united-nations-evolving-privacy-discourse-and-corporate-human-rights; Rotenberg, Marc, Urgent Mandate, Unhurried Response: An Evaluation of the UN Special Rapporteur on the Right to Privacy, 3 Eur. Data Prot. L. Rev. 47, 2017

[29] ECtHR, Roman Zakharov v. Russia, Application no. 47143/06, Judgement of 4 December 2015; ECtHR, Big Brother Watch and Others v. the United Kingdom, Application nos. 58170/13, 62322/14 and 24960/15, Judgement of 13 September 2018; CJEU, Max Schrems v. Data Protection Commissioner, C-362/14, 6 October 2015; CJEU, Data Protection Commissioner v. Facebook & Max Schrems, C-311/18, 16 July 2020

[30] See Lubin, Asaf, The Liberty to Spy, 61(1) Harv. Int'l L.J. 185 (2020). Available at SSRN: https://ssrn.com/abstract=3327505, p. 221 citing Shany, Yuval, On-Line Surveillance in the Case-law of the UN Human Rights Committee, Hebrew Univ. Cyber Sec. Research Ctr. (July 2017), https://perma.cc/BW4H-K55R

[31] American Civil Liberties Union, Informational Privacy in the Digital Age, February 2015, https://www.aclu.org/other/human-right-privacy-digital-age; Privacy International, Guide to International Law and Surveillance 2.0, February 2019, https://privacyinternational.org/sites/default/files/2019-04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf

[32] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ 2016 L 119/1, https://gdpr-info.eu/, https://gdpr-info.eu/issues/

Article 1 (15) of GDPR defines "data concerning health" as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[33] Article 9 of GDPR prohibits processing of "data concerning health," unless such processing is justified on one of the ten listed grounds,[34] including, among others, explicit consent, protecting vital interests of the data subject, and the public interest in the area of public health.

In principle, the collection and processing of health data is subject to the same criteria for limitations as apply to other privacy interferences. It still requires assessing the necessity and proportionality of the measures imposed, as well as the adequacy of their legal basis. However, the language of GDPR makes it clear that the particular sensitivity of health data requires a higher degree of scrutiny when assessing if health data collection is permissible.

There is, however, an important disclaimer. Although personal health data is confidential and warrants a high degree of protection from unlawful interference, the use of surveillance remains central in responding to public health emergencies. According to the World Health Organization, public health surveillance is the ongoing, systematic collection, analysis, and interpretation of health-related data essential to planning, implementation, and evaluation of public health practice.[35] It is imperative for states to make depersonalized statistical data on a pandemic (such as the number of registered cases and mortality rates) available to the public. This type of surveillance, in contrast to individualized contact-tracing, is not the focus of the present paper because it does not directly affect individual liberties or threaten to disclose personal data.[36]

2. Digital Surveillance Measures Used in the Context of COVID-19

The surveillance employed during the COVID-19 pandemic has taken various forms. The key categories of surveillance analyzed infra are mobile applications and physical surveillance.

2.1. Mobile applications

A diversity of mobile applications have been widely introduced throughout the pandemic.[37] Some are launched by governments or regional authorities, others by private companies. Some are voluntary and some are obligatory. Some apps are based on open protocol technologies, others on closed protocol ones.[38] Even within more transparent open protocols, some use a centralized reporting server (PEPP-PT), while others are decentralized (DP-3T, COCOVID).[39] Some apps are aimed at tracing the contacts of infected individuals, others to control the enforcement of stay-at-home orders.

---

[33] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ 2016 L 119/1, Article 1 (15)

[34] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ 2016 L 119/1, Article 9

[35] Centers for Disease Control and Prevention, FAQ: COVID-19 Data and Surveillance, 3 June 2020, https://www.cdc.gov/coronavirus/2019-ncov/covid-data/faq-surveillance.html

[36] While even anonymized data may be subject to cyber vulnerabilities, the risk of data being stolen or leaked as a result of cyber intrusion by third parties remains largely a question of data security, rather than data privacy. In this case, the collection of data itself is not aimed at violating privacy rights, but the lack of sufficient cybersecurity measures may lead to a privacy breach. In contrast, the present paper focuses on digital surveillance, which directly targets personal data.

[37] Elliot Alderson blog, Covid19 Tracker Apps, https://fs0c131y.com/covid19-tracker-apps/

[38] Safesmart, Open and Closed Protocols – What Does It All Mean?, 23 June 2015, https://safesmart.co.uk/open-closed-protocols-mean/

[39] Ibid.; Paul Schwartz, Protecting privacy on COVID-19 surveillance apps, IAPP, 8 May 2020, https://iapp.org/news/a/protecting-privacy-on-covid-surveillance-apps/

Singapore was a pioneer in launching the "TraceTogether" app in March, which was then outsourced and used by other countries to model their own apps. Singaporean authorities are now supplementing the app with wearable devices to track the spread of the virus more effectively.[40]

China was the first country to face the pandemic and one of the first to resort to technological means of containing it. The Alipay Health Code app is the product of cooperation between the Hangzhou local government and Ant Financial, a sister company of the e-commerce giant Alibaba.[41] It was launched in Hangzhou in early February and rapidly spread across the country. The app assigns users a color code based on one's health status and travel history, which can be scanned by authorities.[42] Generally people with a green code are allowed to travel relatively freely, a yellow code indicates that the holder should be in home isolation, and a red code says the user is a confirmed COVID-19 patient and should be in quarantine.[43] According to The New York Times, as a user grants the software access to personal data, a piece of the program labeled "reportInfoAndLocationToPolice" sends the person's location, city name, and an identifying code number to a server, while the app's connection to the police is not announced to users.[44]

The exact algorithms used to determine the epidemiologically "safe" and "unsafe" individuals are not available to the public, sometimes leading to arbitrary changes of the color-coded "safety" status.[45] This casts doubts on the app's effectiveness in achieving the declared goal of containing the virus and raises yet another privacy concern in China. Especially worrisome is the Chinese authorities' rhetoric around keeping the app in use even as the pandemic subsides. Chinese officials have declared that the technology may become an "intimate health guardian" for individuals and are exploring the possibilities of expanding the health code to rank citizens with a "personal health index."[46]

Russian tracking app "Social monitoring," launched by Moscow authorities, is criticized for being predominantly used as a tool for punitive enforcement of the quarantine. The use of the app is mandated for people who have tested positive for COVID-19 or show respiratory disease symptoms. The app gains access to the user's location, calls, camera, network information, sensors, and other data to ensure that people instructed to self-quarantine do not leave their home during the two-week period.[47] The app randomly sends push notifications instructing users to immediately take and send a selfie as a proof of not having left the house without the phone.[48] A failure to respond to a notification, which can arrive as late as midnight, results in an automatic fine of 4,000 rubles (approximately US$56). Failure to install the app also results in a fine. According to Human Rights Watch, as of May 20, 60,000 Moscow residents have installed the app and 53,000 fines have been issued.[49] The "Social monitoring" app and the practice of using it do not only interfere with privacy rights, but place a substantial financial burden on people already affected by the crisis.

---

[40] Sheila Chiang, From TraceTogether App To Wearable Device: Why Contact Tracing Would Not Work In S'pore, Vulcan Post, 9 June 2020, https://vulcanpost.com/701007/why-contact-tracing-would-not-work-singapore/; Saira Asher, TraceTogether: Singapore turns to wearable contact-tracing Covid tech, BBC News, 4 July 2020, https://www.bbc.com/news/technology-53146360
[41] 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, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[42] Davidson, Helen, China's coronavirus health code apps raise concerns over privacy, The Guardian, 1 April 2020, https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy
[43] Davidson, Helen, China's coronavirus health code apps raise concerns over privacy, The Guardian, 1 April 2020, https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy
[44] 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, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[45] Ibid.
[46] Zhong, Raymond, China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears, The New York Times, 26 May 2020, https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html
[47] Human Rights Watch, Russia: Intrusive Tracking App Wrongly Fines Muscovites, 21 May 2020, https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites
[48] Ibid.
[49] Ibid.

In France, civil liberties groups are concerned with tracing apps leading to government surveillance, despite the French government saying that the "StopCovid" app does not record users' location and destroys data after 14 days.[50] The development of "ProteGO Safe" contact-tracing app in Poland has stirred controversy even among its own developers. Deutsche Welle reported that one of the team members working on the app left the project at an early stage after meeting with the Ministry of Digital Affairs representatives. He claims that "the officials wanted the app to link the data with users' mobile phone numbers, which could enable simple deanonymization of users," a non-negotiable red line for the former app developer.[51] Norway's government halted the use of its contact-tracing app after the country's data-protection authority raised alarms, prioritizing privacy over potential benefits of increased surveillance.[52]

Although concerns about "handing over too much power to foreign tech giants"[53] persist, European governments are mindful of the GDPR's "privacy by design" principle.[54] The German "Corona-Warn-App," for example, does not detect user locations, which means no authorities can spy on the users. The app recognizes only which other app users are currently in the vicinity. This works via Bluetooth, a wireless standard that enables devices to exchange data at close range.[55] The Czech app "eRouška" does not track and collect location information, but only anonymously detects which other users of the application you have come into close contact with.[56] Despite a more privacy-oriented attitude among European countries and consolidated data privacy standards embodied in the GDPR, coronavirus warning apps remain individual national programs, and lack compatibility on the EU level.[57]

Mobile applications continue to be developed and rolled out in dozens of countries worldwide—from highly controversial ones in India[58] or Iran[59] to more privacy-oriented ones in South Africa[60] or Austria.[61] Moreover, pre-COVID data collection and data transfer have never ceased and, if anything, have been used more actively during the pandemic. Mobile applications and related technologies need not be COVID-specific to be employed for the same data collection purposes as the newly introduced apps. The data can be collected through services already in place, e.g., through bulk collection of location data.[62] In some instances the data collection procedures are performed by secret services, undermining

---

[50] Sylvie Corbet and Kelvin Chan, France Launches Contact-Tracing App Despite Privacy Concerns, Voice of America, 4 June 2020, https://learningenglish.voanews.com/a/france-launches-contact-tracing-app-despite-privacy-concerns/5447659.html
[51] Malgorzata Fraser, Coronavirus contact tracing reignites Polish privacy debate, DW, 30 May 2020, https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913
[52] Alexander Martin, Coronavirus: Norway to delete all data collected from its contact-tracing app, Sky News, 15 June 2020, https://news.sky.com/story/coronavirus-norway-to-delete-all-data-collected-from-its-contact-tracing-app-12007226
[53] Jason Horowitz and Adam Satariano, Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation, The New York Times, 16 June 2020, https://www.nytimes.com/2020/06/16/world/europe/contact-tracing-apps-europe-coronavirus.html
[54] https://gdpr-info.eu/issues/privacy-by-design/
[55] Fabian Schmidt, German COVID-19 warning app wins on user privacy, DW, 15 June 2020, https://www.dw.com/en/german-covid-19-warning-app-wins-on-user-privacy/a-53808888; Privacy International, "Germany copies Singapore's TraceTogether app for contact tracing," 24 March 2020, https://privacyinternational.org/examples/3566/germany-copies-singapores-tracetogether-app-contact-tracing
[56] Raymond Johnston, Smartphone app eRouška will track potential contacts with coronavirus carriers, ExpatsCz, 15 April 2020, https://news.expats.cz/weekly-czech-news/smartphone-app-erouska-will-track-potential-contacts-with-coronavirus-carriers/
[57] Fabian Schmidt, German COVID-19 warning app wins on user privacy, DW, 15 June 2020, https://www.dw.com/en/german-covid-19-warning-app-wins-on-user-privacy/a-53808888
[58] Patrick Howell O'Neill, India is forcing people to use its covid app, unlike any other democracy, MIT Technology Review, 7 May 2020, https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/
[59] David Gilbert, Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People, Vice News, 14 March 2020, https://www.vice.com/en_us/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people
[60] Luis Monzon, SA Government, UCT Partner on COVID-19 Tracing App, IT News Africa, 30 April 2020, https://www.itnewsafrica.com/2020/04/sa-government-uct-partner-on-covid-19-tracing-app/
[61] Gernot Fritz and Boris Klimpfinger, Contact tracing apps in Austria: a Red Cross initiative, Freshfields Bruckhaus Deringer, 30 April 2020, https://digital.freshfields.com/post/102g62d/contact-tracing-apps-in-austria-a-red-cross-initiative, "Data protection audits by universities and non-profit organizations (including Max Schrems' NYOB) have assessed the app as being 'data protection friendly' to a large extent."
[62] Human Rights Watch, Mobile Location Data and Covid-19: Q&A, 13 May 2020, https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa

the transparency of data collection processes, for example, in Israel, where the Israeli secret service, Shin Bet, collected data about infected individuals and their contacts.[63]

2.2. Physical surveillance

Cameras and drones are an even more tangible instrument of COVID-related "biopolitics."[64] The (often intimidating) presence of cameras in public spaces has already been controversial pre-pandemic. However, the opportunistic attitude of some actors to enhance the capabilities of video surveillance in times of the pandemic threatens to normalize privacy-intrusive practices.

According to media reports, drone surveillance has been deployed in the United States,[65] Mexico,[66] Malaysia,[67] Spain,[68] Italy,[69] and the UK.[70] Camera surveillance has been used in France,[71] Russia,[72] China,[73] and the United States.[74] The Electronic Frontier Foundation (EFF) characterized the use of drone surveillance to fight COVID-19 as "the slipperiest of all slopes."[75] According to EFF, "if police now start to use drones to identify people who are violating quarantine and walking around in public after testing positive for COVID-19, police can easily use the same drones to identify participants in protests or strikes once the crisis is over." [76] Similar concerns have been raised by Human Rights Watch regarding the use of outside surveillance cameras in Moscow, Russia. The organization stated that

---

[63] Stuart Winer and Toi Staff, High Court: Shin Bet surveillance of virus carriers must be enshrined in law, The Times of Israel, 26 April 2020, https://www.timesofisrael.com/high-court-shin-bet-surveillance-of-virus-carriers-must-be-enshrined-in-law/

[64] Biopolitics is a term coined by Michel Foucault and meaning "a power that exerts a positive influence on life, that endeavors to administer, optimize, and multiply it, subjecting it to precise controls and comprehensive regulations." See Michel Foucault, The Will to Knowledge: The History of Sexuality, Volume 1, Pantheon Books: New York, 1976 (translated by Robert Hurley, 1998), p. 137. In the COVID-19 surveillance context, the biopolitics of controlling populations manifests in "tracking the movements of individuals, mandating checking in and registration on arrival or on entering mass events, or by way of outsourcing surveillance to the technology companies." See Ignas Kalpokas, The Biopolitics of Covid-19: The Pure Governmentality of Life, European Consortium for Political Research, August 2020, https://ecpr.eu/Filestore/paperproposal/a393fb94-1c69-458a-8d94-96d47f9309ec.pdf.

[65] Henry Shwan, Drones in Florida Remind Residents to Keep Their Social Distance, Governing, 15 April 2020, https://www.governing.com/now/Drones-in-Florida-Remind-Residents-to-Keep-Their-Social-Distance.html; Adam K. Raymond, Social Distancing Enforcement Drones Arrive in the U.S., Intelligencer, 8 April 2020, https://nymag.com/intelligencer/2020/04/social-distancing-enforcement-drones-arrive-in-the-u-s.html; Dan Krauth, Coronavirus News: Pandemic drones to monitor fever, crowds from above, Eyewitness News, 15 April 2020, https://abc7ny.com/coronavirus-drones-covid-19-pandemic-nj/6102905/; April Glaser, Homeless people are at risk from the coronavirus. Police have a contentious solution: Drones, NBC News, 24 April 2020, https://privacyinternational.org/examples/3775/us-law-enforcement-uses-drones-communicate-homeless-encampments

[66] Privacy International, Mexico: Municipality uses drones to enforce lockdown rules, 24 march 2020, https://privacyinternational.org/examples/3562/mexico-municipality-uses-drones-enforce-lockdown-rules

[67] Opalyn Mok, Authorities monitor MCO-compliance from the sky with drones, Malaymail, 24 March 2020, https://www.malaymail.com/news/malaysia/2020/03/24/authorities-monitor-mco-compliance-from-the-sky-with-drones/1849681

[68] Charlie Wood, Spanish police warn lockdown violators via drones and remote radio, Business Insider, 16 March 2020, https://www.businessinsider.com/spanish-police-using-drones-to-ask-people-stay-at-home-2020-3

[69] Luca Santocchia, Italian mayor uses drone to scream at locals to stay indoors amid coronavirus crisis, Euronews, 27 March 2020, https://www.euronews.com/2020/03/26/watch-italian-mayor-uses-drone-to-scream-at-locals-to-stay-indoors-amid-coronavirus-crisis

[70] BBC News, Coronavirus: Peak District drone police criticised for 'lockdown shaming,' 27 March 2020, https://www.bbc.com/news/uk-england-derbyshire-52055201

[71] Chloe Hadavas, France Is Using A.I. to Detect Whether People Are Wearing Masks, Slate, 8 May 2020, https://slate.com/technology/2020/05/france-artificial-intelligence-mask-detection-coronavirus.html

[72] Sam Ball, 100,000 cameras: Moscow uses facial recognition to enforce quarantine, France 24, 24 March 2020, https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine; Roskomsvoboda, Spying through "Quarantine," 13 May 2020, https://roskomsvoboda.org/58309/; Roskomsvoboda, The authorities are using facial recognition system under the pretense of fighting COVID-19, 13 May 2020, https://roskomsvoboda.org/56476/

[73] Arjun Kharpal, Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends, CNBC, 26 March 2020, https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html; Nectar Gan, China is installing surveillance cameras outside people's front doors ... and sometimes inside their homes, CNN Business, 28 April 2020, https://www.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html

[74] Joseph Cox, Surveillance Company Says It's Deploying 'Coronavirus-Detecting' Cameras in US, Vice, 17 March 2020, https://www.vice.com/en_us/article/epg8xe/surveillance-company-deploying-coronavirus-detecting-cameras ; Matthew Guariglia and Cooper Quintin, Thermal Imaging Cameras are Still Dangerous Dragnet Surveillance Cameras, Electronic Frontier Foundation, 7 April 2020, https://www.eff.org/deeplinks/2020/04/thermal-imaging-cameras-are-still-dangerous-dragnet-surveillance-cameras

[75] Matthew Guariglia, Using Drones to Fight COVID-19 is the Slipperiest of All Slopes, Electronic Frontier Foundation, 5 May 2020, https://www.eff.org/deeplinks/2020/05/using-drones-fight-covid-19-slipperiest-all-slopes

[76] Ibid.

"Russia's enthusiasm for surveillance before the pandemic gives rise to concern that its expanded use to fight COVID-19 might not end after the pandemic is over."[77]

The proposed use of thermal imaging cameras, designed to detect fever from a distance and marketed as a narrow COVID-tailored measure, has also faced criticism from digital rights activists, maintaining that "thermal cameras are still surveillance cameras." According to EFF, acquiring and installing "fever detection" cameras "increases the likelihood that the hardware will long outlive its usefulness during this public health crisis," producing a chilling effect on free expression, movement, and association, aiding in the targeted harassment and over-policing of vulnerable populations, and opening the door to face recognition.[78]

Indeed, what makes the use of physical surveillance even more troubling from the privacy standpoint is the potential to integrate it with facial recognition technologies[79]—a practice already adopted by some states.[80] Facial recognition technologies have attracted close attention of the media and politicians recently. U.S. Senator Edward Markey, for example, expressed concern about facial recognition as a tool of combating the pandemic and warned that COVID-19 contact tracing should not be "used as cover by companies … to build shadowy surveillance networks."[81] Similar concerns are shared by digital rights activists, who believe that although "public health crises may require extraordinary measures in favor of the public good," it is not in the public's interest to resort to invasive face surveillance. [82]

The pitches of Clearview AI—a start-up known for developing facial recognition technologies—go beyond the promise of controlling the spread of the pandemic by appealing primarily to law enforcement agencies, who are encouraged to embrace the technology to effectively investigate and punish crime.[83] Normalization of facial recognition as a long-term tool of law enforcement continues to face severe criticism. [84]

Even presuming the best intentions of putting facial recognition technology to an admirable use as an anti-pandemic tool, it is hardly possible to prevent the transportation of this surveillance tool into less noble realms. Pre-pandemic facial recognition technologies were a major threat in recent Hong Kong protests, pushing the protesters to use masks and conceal their faces to avoid being detected and

---

[77] Nicola Habersetzer, Moscow Silently Expands Surveillance of Citizens, Human Rights Watch, 25 March 2020, https://www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens

[78] Matthew Guariglia and Cooper Quintin, Thermal Imaging Cameras are Still Dangerous Dragnet Surveillance Cameras, Electronic Frontier Foundation, 7 April 2020, https://www.eff.org/deeplinks/2020/04/thermal-imaging-cameras-are-still-dangerous-dragnet-surveillance-cameras

[79] Lindsey O'Donnell, COVID-19 Spurs Facial Recognition Tracking, Privacy Fears, ThreatPost, 20 March 2020, https://threatpost.com/covid-19-spurs-facial-recognition-tracking-privacy-fears/153953/; Matthew Guariglia, Face Surveillance Is Not the Solution to the COVID-19 Crisis, Electronic Frontier Foundation, 19 March 2020, https://www.eff.org/deeplinks/2020/03/face-surveillance-not-solution-covid-19-crisis

[80] Nicola Habersetzer, Moscow Silently Expands Surveillance of Citizens, Human Rights Watch, 25 March 2020, https://www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens

[81] Alfred Ng, Lawmakers propose indefinite nationwide ban on police use of facial recognition, CNET, 25 June 2020, https://www.cnet.com/news/lawmakers-propose-indefinite-nationwide-ban-on-police-use-of-facial-recognition/; Jacob Ward and Chiara Sottile, A facial recognition company wants to help with contact tracing. A senator has questions, NBC News, 30 April 2020, https://www.nbcnews.com/tech/security/facial-recognition-company-wants-help-contact-tracing-senator-has-questions-n1197291

[82] Matthew Guariglia, Face Surveillance Is Not the Solution to the COVID-19 Crisis, Electronic Frontier Foundation, 19 March 2020, https://www.eff.org/deeplinks/2020/03/face-surveillance-not-solution-covid-19-crisis

[83] Kashmir Hill, The Secretive Company That Might End Privacy as We Know It, The New York Times, 18 January 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[84] Georgetown Law Center on Privacy and Technology, The Perpetual Line-Up: Unregulated Police Face Recognition in America, 18 October 2016, https://www.perpetuallineup.org/

persecuted.[85] With masks becoming the new normal, technology is being adapted to allow facial recognition to identify individuals even if they are wearing masks.[86]

Whether the technology reaches complete accuracy or not, the consequences are equally detrimental. An infallible facial recognition technology with zero mistakes makes it possible to target political opponents and protesters, endangering their privacy even more. A more realistic scenario where facial recognition continues to make occasional mistakes is likely to reflect biases and disproportionately affect minorities.[87]

3. Legal Framework for Regulating COVID-19 Surveillance Practices: Derogations to and Limitations on the Right to Privacy

3.1. Guiding principles and standards

The current pandemic raises both old and new challenges to privacy and has prompted a flurry of expert reports and statements to guide policymakers and legislators as they consider measures to protect public health. A recent joint statement of experts from the United Nations (UN), the Inter-American Commission for Human Rights (IACHR), and the Organization for Security and Co-operation in Europe (OSCE) has cautioned against the invasions of privacy in the name of fighting the COVID-19 pandemic. It states, in relevant part:

"… We are aware of growing use of tools of surveillance technology to track the spread of the coronavirus. While we understand and support the need for active efforts to confront the pandemic, it is also crucial that such tools be limited in use, both in terms of purpose and time, and that individual rights to privacy, non-discrimination, the protection of journalistic sources and other freedoms be rigorously protected. States must also protect the personal information of patients. We strongly urge that any use of such technology abide by the strictest protections and only be available according to domestic law that is consistent with international human rights standards.[88]

Digital rights activists have repeatedly raised similar concerns. In April 2020, for example, 134 international, regional, and local organizations signed a joint civil society statement calling upon states to not use the efforts to contain the virus "as a cover to usher in a new era of greatly expanded systems of invasive digital surveillance."[89] It formulated specific conditions that must be respected when responding to the pandemic with increased surveillance.[90]

The Center for Democracy and Technology also issued a statement "regarding the use of data to fight COVID-19," supported by 15 cybersecurity experts.[91] It identified seven key areas, in which privacy concerns must be balanced with digital responses to the pandemic: efficacy, volition, aggregation,

---

[85] Paul Mozur, In Hong Kong Protests, Faces Become Weapons, The New York Times, 26 July 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html

[86] Susan Miller, Facial recognition adapts to a mask-wearing public, GCN, 3 June 2020, https://gcn.com/articles/2020/06/03/facial-recognition-masks.aspx; Yuan Yang, How China built facial recognition for people wearing masks, ArsTechnica, 18 March 2020, https://arstechnica.com/tech-policy/2020/03/how-china-built-facial-recognition-for-people-wearing-masks/

[87] Drew Harwell, Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use, The Washington Post, 19 December 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/; Kashmir Hill, The Secretive Company That Might End Privacy as We Know It, The New York Times, 18 January 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[88] Joint Statement by David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Harlem Désir, OSCE Representative on Freedom of the Media, and Edison Lanza, IACHR Special Rapporteur for Freedom of Expression, COVID-19: Governments must promote and protect access to and free flow of information during pandemic – International experts, 19 March 2020, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E

[89] Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights, 2 April 2020, https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf

[90] Below is the redacted and shortened version of the conditions.

[91] Center for Democracy and Technology, Statement Regarding the Use of Data to Fight COVID-19, 30 April 2020, https://cdt.org/wp-content/uploads/2020/04/CDT-Statement-Regarding-Use-of-Data-to-Fight-COVID-19.pdf

consequences, transparency, fairness, and duration.[92] The Electronic Privacy Foundation and a group of over 80 consumer, privacy, civil rights, and civil liberties organizations called upon the United States House and the Senate to endorse "principles to protect the civil rights and privacy of all persons."[93]

In his 2020 report on disease pandemics, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye formulated six principles that should govern surveillance in the pandemic that echo many of those formulated by digital rights activists:

1. *Any authorization of surveillance should be contained in precise and publicly accessible laws and only be applied when necessary and proportionate to achieve a legitimate objective (such as protecting public health);*
2. *Authorization of surveillance of specified individuals should be based on independent evaluation, preferably by a judicial authority, with appropriate limitations on time, location, manner and scope;*
3. *Rigorous record-keeping should be required so that individuals and oversight bodies can ascertain that surveillance was conducted for legitimate public health purposes;*
4. *Any personal data collected should be subject to strict privacy protections to ensure against disclosure of personal information to anyone not authorized for public health purposes;*
5. *Some personal data should be expressly excluded from collection, such as the content of a person's communications, and robust safeguards must be put in place to ensure against any government or third-party misuse of such data, including use for purposes unrelated to the public health emergency;*
6. *Where personal data is anonymized, the State and any third-party actor involved in collection must be able to demonstrate such anonymity.*[94]

The principles, formulated by activists and experts, are not new and rest on the well-established standards of legality, necessity, and proportionality. Some of them highlight the risks, which international law is only partially ready to handle—such as the reliance on private companies for data collection and the correspondent obligation of business as well as governments to respect human rights.[95]

3.2. International legal norms

The first global pandemic of the digital era will once again put privacy commitments of states and companies to the test. Beyond policy and activist rhetoric, the crucial task for rule of law actors worldwide is identifying the black-letter legal standards for protecting privacy, which must be followed whenever surveillance measures are introduced.

Under international human rights law, which enshrines the right to privacy, states have two key legal mechanisms to put their tech-based COVID-19 responses into a legal framework: limitations and derogations. On the universal human rights level, both mechanisms are enshrined in the ICCPR.[96] Similar

[92] Center for Democracy and Technology, Statement Regarding the Use of Data to Fight COVID-19, 30 April 2020, https://cdt.org/wpcontent/uploads/2020/04/CDT-Statement-Regarding-Use-of-Data-to-Fight-COVID-19.pdf
[93] EPIC, EPIC, Coalition to Congress: Tech Responses to Covid-19 Must Protect Privacy & Civil Rights, 11 June 2020, https://epic.org/2020/06/epic-coalition-to-congress-tec.html
[94] United Nations General Assembly, Report of the of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, on disease pandemics and the freedom of opinion and expression, A/HRC/44/49, 23 April 2020, https://undocs.org/A/HRC/44/49
[95] See United Nations, Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework, 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
[96] United Nations, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171, Article 4; The provisions of ICCPR on derogations and limitations are further interpreted in non-binding documents—notably, in the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights adopted by the American Association for the International Commission of Jurists in 1985, https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf

provisions exist in regional human rights treaties.[97] In the new realities of COVID-19, the UN Office of the High Commissioner for Human Rights and the UN Human Rights Committee have been quick to provide additional guidelines on the use of limitations and derogations mechanisms during the pandemic.[98]

In situations of emergency, international human rights law allows states to derogate from certain human rights obligations to the extent necessary in urgent circumstances. The derogation mechanism under ICCPR presupposes the existence of a life-threatening and nation-wide emergency and requires the derogating state to follow certain procedural steps of declaring the derogation. [99] Derogations are seen as a mechanism to be employed in extraordinary circumstances and only for as long as such circumstances continue to prevent states from fully implementing human rights.

The UN Human Rights Committee, which is responsible for authoritative interpretation of the ICCPR, provides for six specific requirements that states must comply with if they want to derogate from their human rights obligations. States must: 1) proclaim a state of emergency; 2) formally notify the UN Secretary General of their intent to derogate; 3) ensure that derogation measures meet strict tests of necessity and proportionality; 4) ensure that derogation measures do not interfere with other international human rights obligations; 5) guarantee that derogation measures are applied in a manner that is not discriminatory; and 6) continue to uphold non-derogable rights.[100]

While the COVID-19 pandemic can clearly qualify as a life-threatening emergency, at least in states most critically affected by the outbreak, the adherence to a derogation mechanism often remains unrealistic for states. Even those states who announce a state of national emergency often do not opt for going through the fairly complicated procedure of derogating from human rights on the international level. Derogations are a useful tool for ensuring that limitations on human rights are time-bound and limited to the pandemic emergency.[101] However, the failure of states to make use of the derogation mechanism does not mean that the pandemic responses, including those affecting privacy rights, are not subject to international human rights law.

In fact, the UN Office of the High Commissioner for Human Rights recommends that states abstain from using the derogation mechanism when possible, stating that "although derogation or suspension of certain rights is permitted when such emergencies are declared, measures suspending rights should be avoided when the situation can be adequately dealt with by establishing proportionate restrictions or limitations on certain rights."[102]

---

[97] Organization of American States, American Convention on Human Rights, 22 November 1969, Article 27; Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, Article 15

[98] United Nations Office of the High Commissioner for Human Rights, Emergency Measures and COVID-19: Guidance, 27 April 2020, **https://www.ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf**; Human Rights Committee, Statement on derogations from the Covenant in connection with the COVID-19 pandemic, CCPR/C/128/2, 30 April 2020, **https://www.ohchr.org/Documents/HRBodies/CCPR/COVIDstatementEN.pdf**

[99] United Nations, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171, Article 4; See also Organization of American States, American Convention on Human Rights, 22 November 1969, Article 27; Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, Article 15

[100] International Justice Resource Center, OHCHR & Human Rights Committee Address Derogations During COVID-19, 29 April 2020, **https://ijrcenter.org/2020/04/29/ohchr-human-rights-committee-address-derogations-during-covid-19/; Human Rights Committee,** Statement on derogations from the Covenant in connection with the COVID-19 pandemic, CCPR/C/128/2, 30 April 2020, **https://www.ohchr.org/Documents/HRBodies/CCPR/COVIDstatementEN.pdf, para. 2**, pp. 1-2

[101] Alan Greene, States should declare a State of Emergency using Article 15 ECHR to confront the Coronavirus Pandemic, Strasbourg Observers, 1 April 2020, **https://strasbourgobservers.com/2020/04/01/states-should-declare-a-state-of-emergency-using-article-15-echr-to-confront-the-coronavirus-pandemic/**

[102] United Nations Office of the High Commissioner for Human Rights, Emergency Measures and COVID-19: Guidance, 27 April 2020, **https://www.ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf**

Putting limitations on non-derogable human rights is another way in which states can manage their COVID-19 responses. The criteria for using limitations is less stringent than those governing derogations. Human rights can be lawfully limited even in times where no pressing life-threatening emergency exists. That does not mean that limitations on human rights have no reasonable boundaries. To the contrary, a set of criteria needs to be met for limitations to be considered lawful.

While the limitations mechanism does not have a dedicated article in ICCPR, it is reflected in various substantive articles of ICCPR[103] and elaborated on in jurisprudence[104] and expert analysis.[105] In the surveillance context, the jurisprudence of the ECtHR[106] is particularly helpful when interpreting the conditions for lawful limitations on privacy since no other international judicial or quasi-judicial body has come close to ECtHR experience in handling surveillance-related cases. The ECtHR criteria for lawful limitations of privacy are also consistent with the ICCPR's treaty body's interpretation of "arbitrary or unlawful" interferences with privacy under Article 17 of ICCPR.[107]

According to these sources, surveillance measures introduced to fight COVID-19 must cumulatively satisfy the following criteria:[108]

1. Legality

   The measures in question must be adopted "in accordance with law." Following the ECtHR approach, this means that surveillance must be clearly sanctioned by domestic law of the State practicing it. However, merely documenting the surveillance measures on paper will not be enough to satisfy this criterion. The law introducing surveillance measures must be "foreseeable" —that is, sufficiently precise "to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any [surveillance] measures."[109] In the COVID-19 context, this means that individuals targeted by surveillance are entitled to know what information about them or their contacts will be collected, who will be able to access the information collected, and what are the limits on data retention.

[103] United Nations, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171, Article 18 (3); Article 19 (3); Article 22 (2). See also Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, https://www.refworld.org/docid/453883f922.html on the definition of "arbitrary or unlawful interference"

[104] See, for instance, ECtHR, Roman Zakharov v. Russia, Application no. 47143/06, Judgement of 4 December 2015; ECtHR, Big Brother Watch and Others v. the United Kingdom, Application nos. 58170/13, 62322/14 and 24960/15, Judgement of 13 September 2018

[105] American Association for the International Commission of Jurists, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 1985, https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf, pp. 6-9

[106] See, for instance, ECtHR, Liberty and Others v. the United Kingdom, Application no. 58243/00, Judgement of 1 July 2008; ECtHR, Kennedy v. the United Kingdom, Application no. 26839/05, Judgement of 18 May 2010; ECtHR, Roman Zakharov v. Russia, Application no. 47143/06, Judgement of 4 December 2015; ECtHR, Big Brother Watch and Others v. the United Kingdom, Application nos. 58170/13, 62322/14 and 24960/15, Judgement of 13 September 2018. Transatlantic data flows between the EU and the US have also been scrutinized by the Court of Justice of the European Unions in Schrems 1 and 2 cases. See CJEU, Max Schrems v. Data Protection Commissioner, C-362/14, 6 October 2015; CJEU, Data Protection Commissioner v. Facebook & Max Schrems, C-311/18, 16 July 2020

[107] Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, https://www.refworld.org/docid/453883f922.html

[108] Office of the United High Commissioner for Human Rights, Report on the Right to Privacy in the Digital Age, A/HRC/27/37, 30 June 2014, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[109] ECtHR, Big Brother Watch and Others v. the United Kingdom, Application nos. 58170/13, 62322/14 and 24960/15, Judgement of 13 September 2018, para. 306, p. 127

2. Necessity

The necessity criterion implies that any surveillance measures must address a "pressing social need."[110] While there is hardly a disagreement as to whether COVID-19 pandemic would qualify as such, the necessity of keeping surveillance measures in place post-COVID to prevent future pandemics can be more debatable.

3. Proportionality

The balance between the ends and means of surveillance is critical. If surveillance measures are ineffective in handling the pandemic and detrimental to individual privacy, they would not satisfy the proportionality criterion. Massive privacy intrusions would not be justified by marginal gains in containing the pandemic. The limitations on the right to privacy must represent the least intrusive option among those that might achieve the desired result.[111]

A relevant consideration in assessing the lawfulness of a particular limitation is whether or not such limitation is non-discriminatory. While in the jurisprudence of the ECtHR this aspect is usually addressed as part of a separate violation of Article 14 of the ECHR, it is not uncommon to also treat it as another criterion for lawful limitations on human rights.[112] The limitation is non-discriminatory when it does not unfairly target the representatives of a particular group. However, not targeting a particular demographic in a discriminatory manner should be distinguished from introducing mass surveillance measures that sweep too broadly, sparing no one from intrusion on their privacy.

The application of the lawful limitation test to actual surveillance measures applied during COVID-19 pandemic should be analyzed on a case-by-case basis. The adequacy of safeguards against privacy abuses will depend on a number of factors —how transparent states are about the surveillance measures, how much information is collected, and how helpful the collected data is to actually combat the spread of the virus. To illustrate the range of outcomes, the table below, comparing two different surveillance apps against the three requirements of legality, necessity and proportionality, reflects the kind of case-by-case evaluation that is needed to assess lawfulness of different measures:

[110] United Nations Office of the High Commissioner for Human Rights, Emergency Measures and COVID-19: Guidance, 27 April 2020, https://www.ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf
[111] United Nations Office of the High Commissioner for Human Rights, Emergency Measures and COVID-19: Guidance, 27 April 2020, https://www.ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf
[112] Adina Ponta, Human Rights Law in the Time of the Coronavirus, ASIL Insights, Volume 24, Issue 5, https://www.asil.org/insights/volume/24/issue/5/human-rights-law-time-coronavirus

Surveillance measure	Legality	Necessity	Proportionality
Contact-tracing app A: Introduced before the peak of the pandemic; Introduced in accordance with a public act, jointly issued by the Ministry of Healthcare and the Ministry of Information. The act provides details of permissible data collection collects Bluetooth data to determine the proximity to other app users; Encrypts the collected data; Does not collect GPS data, passport data, social security data; Automatically deletes the collected data after 90 days.	Likely to satisfy the legality criterion. The app was launched based on official governmental act that specifies the modalities of permissible data collection. The more details such act provides on the types of data collected, the measures to secure the data, the terms of data retention, the more likely it is to satisfy the legality criterion. If the act is drafted in vague terms or is not made available to public, it is less likely to satisfy the legality criterion.	Likely to satisfy the necessity criterion. The app was launched before the peak of the pandemic, when the need for preventing the virus spread through contact-tracing was evident and urgent. The more scientific data is available to substantiate the need for a contact-tracing measure, the more likely it is to satisfy the necessity criterion.	Likely to satisfy the proportionality criterion. The app is tailored to the need of performing pandemic-related contact-tracing. It does not collect more information than strictly necessary to achieve the declared goal. It only collects Bluetooth data of the users' phones and users' phone numbers, without targeting GPS data, passport or social security numbers, health records, etc. It also encrypts the collected data and only stores it for 90 days. The more tailored the data collection is to achieve the goal of tracing the spread of the pandemic, the more likely it is to satisfy the proportionality criterion.
Contact-tracing app B: Introduced after the peak of the pandemic, when the number of cases was proven to be consistently decreasing; Introduced based on a Secret Service act, the contents of which are classified and unpublished. Only limited information is available to the public; Collects GPS data to track the whereabouts of all citizens, passport number, and social security number; does not encrypt the collected data; Stores the collected data for 10 years.	Unlikely to satisfy the legality criterion. The app was launched based on a secret act, which was not made available to the public. Merely the existence of an official act under which the surveillance is performed is not enough to satisfy the legality criterion if individuals are not informed about the specific surveillance measures applicable to them.	Unlikely to satisfy the necessity criterion. The app was launched after the peak of the pandemic when the number of cases was consistently dropping. At that stage of the pandemic the need for introducing surveillance measures is not evident. While contact-tracing may be justified even at post-pandemic stage, the absence of a pressing social need for contact-tracing may render the app unlawful.	Unlikely to satisfy the proportionality criterion. The app collects more information than necessary to achieve the declared goal. The app collects personal data, including passport number, social security number, and exact GPS location. The data is unencrypted and stored for 10 years after collection, when the pandemic is likely to subside. Overly broad surveillance measures that target more information than necessary to slow the spread of the pandemic are unlikely to satisfy the proportionality criterion.

Whether states adopt a derogations or limitations framework (with the latter still being a more realistic option), their surveilling powers will not be absolute. To prevent illegitimate privacy intrusions, an assessment like the one above should become a centerpiece in analyzing whether particular surveillance measures are compliant with international human rights law.

Conclusion

Emergency situations, as unpredictable and destructive as they are, should not be used as windows of opportunity to weaken states' obligations to respect fundamental rights. The attempts to enhance surveillance measures to the detriment of privacy should be met with scrutiny and skepticism. The rhetoric of "extreme times requiring extreme measures" may be easily used to justify Orwellian approaches of handling the pandemic. Legal scholar Alan Rozenshtein has warned about the dangers of "surveillance creep," stating that "pandemics, like other emergencies, have often been these catalyst moments for the permanent expansion of the government, [and] the government does not tend to shrink after the moment has passed."[113]

Perhaps, it is indeed naive to think that "once the smoke has cleared," the surveillance will cease completely. After all, the practice of mass electronic surveillance was a pressing issue long before COVID-19. The pre-pandemic world, as famously revealed by Edward Snowden, was far from a privacy haven. The post-pandemic world may escalate privacy concerns even further.

States and corporate entities seizing momentum to test their surveillance capabilities should be held accountable to human rights standards of legality, necessity, and proportionality. The transparency and oversight of surveillance measures by domestic and international actors is crucial. The inherently false trade-off between privacy and health, where only one option could be chosen, should be rejected. Citizens should not settle for anything less than a fully effective pandemic surveillance system that respects privacy.

International human rights law guarantees do not cease in times of a pandemic. They are designed to remain applicable in various scenarios while giving states the necessary discretion to balance privacy concerns with the objective need to collect information. International human rights law already provides states with a toolkit of derogations from and limitations of the right to privacy. States resorting to tech-based surveillance measures during the pandemic are expected to use this toolkit responsibly—in full compliance with both substantive and procedural requirements. Any potentially privacy-intrusive measure must have a sound basis in law and be tailored to the declared goal of combating the pandemic.

The rule of law in any given country rests on the notion of trust in the government. The ability to handle a public health emergency without sliding into a surveillance state panopticon is an essential foundation for such trust. Decisions states are currently making on how to proceed in fighting this digital age pandemic will undoubtedly shape the rule of law landscape for years to come.

[113] Mike Giglio, Would You Sacrifice Your Privacy to Get Out of Quarantine?, The Atlantic, 22 April 2020, https://www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172/