European Center for Not-for-Profit Law

INCLO
INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

PRIVACY INTERNATIONAL

Under Surveillance: (Mis)use of Technologies in Emergency Responses

Global lessons from the Covid-19 pandemic

Contents

Introduction

Project background

In the months following the World Health Organization's declaration of a Public Health Emergency of International Concern on January 30, 2020, more than half the world's countries enacted emergency measures in response to the Covid-19 pandemic. With these emergency measures came **increases in executive powers, suspensions of the rule of law and an upsurge in security protocols** – with subsequent impacts on fundamental human rights, including freedoms of expression, assembly, association, privacy and movement, among others. According to UN Secretary General António Guterres, **some governments used the pandemic as a convenient pretext to further their own political aims**, introducing emergency security measures to "crush dissent, criminalise basic freedoms, silence independent reporting and restrict the activities of nongovernmental organisations." The impact of these emergency measures on civic space has already been well documented by UN special procedures, regional multilateral bodies, human rights defenders and civil society organizations.

Within this broader context of shrinking civic space as a result of emergency measures, we have seen a **rapid and unprecedented scaling up of governments' use of technologies to enable widespread surveillance**. These technologies include contact-tracing and quarantine-monitoring apps, drone surveillance, SIM card tracking, electronic wristbands, biometric technologies, such as facial recognition technologies, and data scraping of social media for mentions of Covid-19. In some cases, technologies were deployed in conjunction with legal measures to criminalize those accused of violating Covid-19 protocols. Surveillance technology was used at the detection stage to identify people who allegedly broke quarantine or spread misinformation about the virus; these people were then penalized under emergency legal measures. As we detail in the report below, many of these technologies were developed and deployed in a non-transparent manner, without legal frameworks, appropriate accountability and oversight mechanisms, or clear sunset clauses stipulating when they would be phased out.

Surveillance technologies exacerbated the impacts of Covid-19 emergency measures on civic space by allowing governments to collect fine-grained data about individuals while also working across large scales of information, in a way that has been unprecedented in the history of global pandemics. We view these technologies as **enablers** that allowed states to carry out emergency measures like social distancing and mandatory lockdown (sometimes to the detriment of the freedom of assembly) and **accelerators** that made emergency responses more efficient and yet more intrusive, infringing, for example, the right to privacy. As this report will show, these immensely powerful and increasingly ubiquitous technologies had and continue to have very serious implications for the enjoyment of human rights – and for civic space more broadly.

Project scope

To combat rising authoritarianism, the **Emergency Powers Coalition**, a collective of civil society organizations globally, is taking action to resist and roll back emergency powers in national laws and strengthen standards in international fora. As part of this effort, the European Center for Not-for-Profit Law (ECNL), the International Network of Civil Liberties Organizations (INCLO) and Privacy International (PI) joined together to track the negative impacts of surveillance technology and measures employed during the Covid-19 pandemic on activist movements and organizations. This report provides key findings of this research and recommendations to ensure more human rights-centered technological responses to future emergencies.

We conducted a broad survey of Covid-19 surveillance measures adopted in **15 countries where INCLO members operate** and, with the help of research partners on the ground, **took a deep dive into six countries** – Colombia, France, India, Indonesia, Kenya and South Africa – using representative examples from these countries of the measures taken during the pandemic. Though our case studies focused on these six countries, the impact of Covid-19 surveillance measures is truly global. We found evidence of their use around the world, from democracies to more authoritarian states, on all six inhabited continents.

Introduction

In conducting research for this report, we sought to understand what actually occurred after the surveillance measures were first introduced, beyond the initial wave of media coverage. We investigated the following questions, considering also broader Covid-19 measures and the context of the political and civic spaces in selected countries:

1. What has happened since the surveillance measures were first introduced?
2. What have the impacts been?
3. How have different groups in society been affected? Have any demographic groups been more affected than others?
4. Are the surveillance measures still in place? Or have they been repealed/rescinded?
5. Has there been resistance, litigation or advocacy in response to pandemic-related surveillance? What can we learn from these actions?

We identified five **overarching trends, namely:**

1. the repurposing of existing security measures;
2. the silencing of civil society;
3. the risk of abuse of personal data;
4. the influential role of private companies; and
5. the normalization of surveillance beyond the pandemic.

In this report, we elaborate on each of these issues, provide illustrative examples and analyse the associated threats to fundamental human rights, including freedom of association and assembly, the right to privacy and freedom of movement. We recognize that this mapping exercise does not capture all possible impacts of surveillance measures adopted during the pandemic. Nevertheless, we hope it will contribute a vital civic space perspective to the discussion about technological responses to future emergencies and necessary human rights safeguards.

We acknowledge that the Covid-19 pandemic is still ongoing and that different countries are at different stages of the pathway to recovery. The cases and analyses presented in this report are concerned with a discrete period of the pandemic from January 2020 to October 2022. Though many of the surveillance measures introduced at the beginning of the pandemic have now been suspended, the situation will require continuous monitoring before we can understand its long-term impact on civil society.

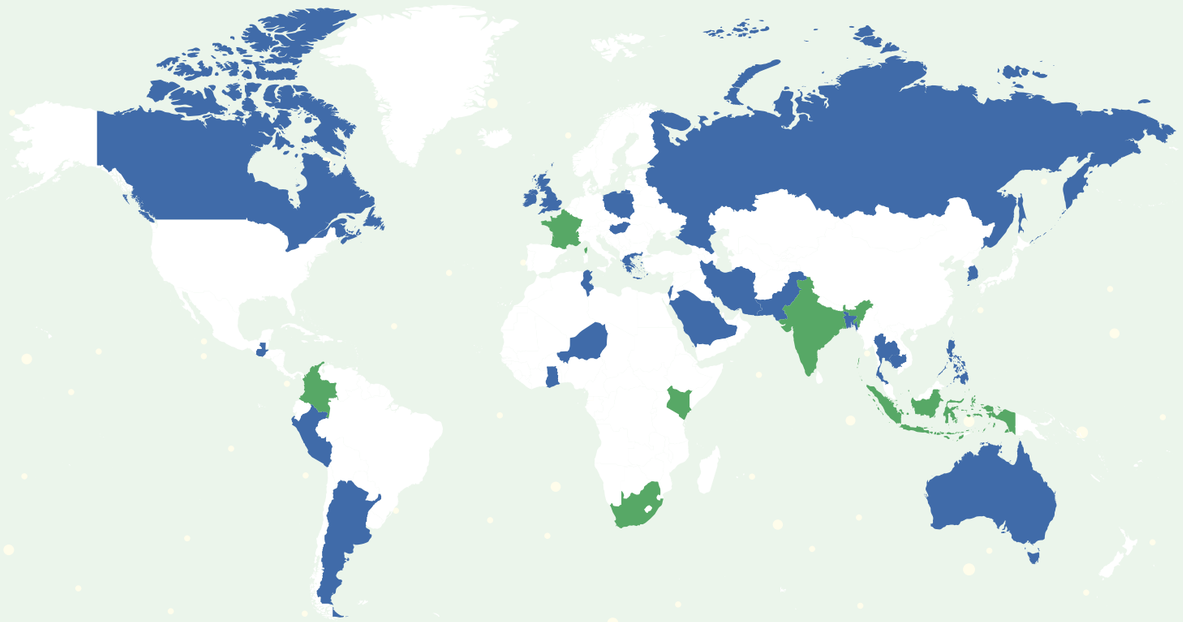

Figure 1. The map illustrates, in green, the countries where we conducted in-depth case studies and, in blue, other countries mentioned in the report.

Methodology

The methodology for this study included:

- Desk research and analysis of policy documents, media reports and white papers;
- A survey sent to the member organizations of INCLO, representing civil society in 15 countries;
- Locally specific research conducted by partner organizations in Colombia, France, India, Indonesia, Kenya and South Africa;
- Synthesis and analysis of reports submitted by partner organizations; and
- Discussion of key findings and trends across countries during meetings of the entire international project team.

Trend 1: Repurposing of existing security measures

In order to quickly roll out Covid-19 surveillance measures, **some governments took advantage of existing frameworks and resources that had originally been introduced for counter-terrorism efforts**, including drawing upon existing legislation, deploying military technologies, and calling upon national intelligence services. This kind of repurposing was encouraged by the private sector. A Reuters investigation identified "at least eight surveillance and cyber-intelligence companies attempting to sell **repurposed spy and law enforcement tools**" to governments by repackaging their products as tools for tracking the virus and enforcing quarantines. We observed an overall trend in which laws, technologies and agencies that had previously been associated with counter-terrorism and national security pivoted to the new objective of fighting the spread of Covid-19.[1]

Targeting government critics with repurposed cybercrime laws

Cybercrime laws were used during the pandemic to justify surveillance of online activity and the spread of information about the virus. For instance, Niger's government repurposed its 2019 cybercriminal act, after which a journalist by the name of Mamane Kaka Touda was arrested and detained under the charge of "disseminating data intending to disturb public order" due to a social media post about a suspected case of Covid-19. Similarly, in Saudi Arabia, the government announced that "social media posts that question, or instigate against, the COVID-19 curfew" would be subject to prosecution under the Anti-Cybercrime Law. Freedom House reported that in 2020, a Saudi Arabian man was arrested for sharing "news from unknown sources" about Covid-19. He reportedly faced a five-year prison sentence and an $800,000 fine under the Anti-Cybercrime Law. Cybercrime laws were also invoked against citizens in Bangladesh and Kenya who allegedly spread misinformation about Covid-19.

[1] For more details see the forthcoming report from the UN Special Rapporteur on counter-terrorism and human rights, Fionnuala Ní Aoláin, *Covid-19, Counter-terrorism and Emergency Law.*

In some cases, **governments repurposed cybercrime laws to impose (or threaten to impose) disproportionate penalties and target government critics**. In Indonesia, the Ministry of Communication and Information announced its intention to crack down on Covid-19 related "hoaxes", threatening violators with penalties of up to six years in prison or a fine of up to 1 billion rupiah (more than 60,000 USD) in accordance with the Law on Information and Electronic Transactions (ITE Law). Furthermore, in February 2021, the Indonesian government expanded upon the ITE Law by establishing a Virtual Police Unit to preempt and prevent "potential cybercrimes" by monitoring social media content. In practice, **the Virtual Police issued warnings to social media users who criticized the Indonesian government**, which caused concern among netizens and activists. For instance, one user received a warning after posting a video that critiqued the uneven enforcement of Covid-19 social distancing protocols, juxtaposing the crowds that gathered in East Nusa Tenggara during a presidential visit with videos of street vendors being forced to close their stalls.

The use of cybercrime laws to prosecute those who disseminate controversial information about Covid-19 must be considered within a larger context in which **these same laws are being used to unduly limit freedom of expression and suppress not only dissident voices**, including those of journalists and activists, but also those of people seeking to express their political opinion. For instance, in Saudi Arabia, Salma al-Shehab was recently given a 34-year sentence because she amplified the posts of activists and exiles that called for the release of political prisoners. According to an investigation by *The Guardian*, she "was not a leading or especially vocal Saudi activist," and had only 2,597 followers on Twitter. This case exemplifies how **cybercrime laws can be abused for political censorship on social media platforms that have become important sites of activism and civic engagement**. The Covid-19 pandemic has created another justification for repressive governments to extend these powers and expand the kinds of speech they consider harmful to national security.

HIGHLIGHT FROM KENYA

Criminalizing dissent under the pretext of fighting Covid-19 misinformation

Report by the Kenya Human Rights Commission

The Computer Misuse and Cybercrimes Act, 2018 is a piece of legislation that has been used by the state to **punish bloggers and voices of dissent for allegedly publishing misleading information** about the government's preparedness and response to the Covid-19 pandemic. Anyone who published information about Covid-19 online risked contravening the Act, with sections 23 and 24 of the Act carrying punitive criminal sanctions of two and ten years, respectively.

Human rights experts condemned the unlawful arrest and prosecution under the Act of human rights defender Edwin Mutemi wa Kiama, who criticized the Kenyan government online for borrowing from the International Monetary Fund (IMF) for its Covid-19 response, amid frustration with Kenya's debt burden and corruption. Kiama's arrest is part of a worrying trend that has seen the misapplication of the Computer Misuse and Cybercrimes Act, 2018 to disproportionately police freedom of expression. Following numerous interventions by civil society actors, Kiama was unconditionally released on 20 April, 2021 due to lack of sufficient evidence to demonstrate that he had violated certain provisions within this repressive piece of legislation. Throughout the pandemic, the government continued to weaponize this Act to stifle freedom of speech.

More powers for intelligence services

Another trend in pandemic-related surveillance was **national intelligence services receiving special authorization to carry out domestic surveillance activities**. For instance, the Israeli government called upon its secret service agency, Shin Bet, in its fight against the pandemic. In March 2020, Prime Minister Benjamin Netanyahu announced that he had granted authority to Shin Bet intelligence services to retrace the movements of infected patients in order to discover with whom they had come into contact. This retroactive search required security agents to tap into what the *New York Times* called "a vast and previously undisclosed trove of cellphone data" that had been covertly gathered with the aim of countering terrorism. In other words, Netanyahu's response to the pandemic revealed new information about the scope of mass surveillance by Israeli intelligence services, which extends to every single cellphone user in the country. The High Court of Israel quickly condemned this practice.

In Pakistan, the government retrofitted a system that had originally been developed for counter-terrorism purposes by its Inter-Services Intelligence (ISI) directorate, a military spy agency, for the new purpose of monitoring the spread of Covid-19. While the exact mechanism that powered this system is unknown, it appears that a tool which had been originally designed to track terrorists based on cellular geolocation data was repurposed to trace Covid-19 cases. The use of national security tools for civilian purposes and the increased reliance on the ISI raises concerns because human rights defenders have accused the military spy agency of "grave human rights violations", including the torture and killing of journalists, anti-military critics and political activists. According to Pakistani digital rights advocate Hija Kamran, "The ISI's involvement in track and trace, the lack of information regarding the technology or method they are using to monitor and track suspected patients, and the push to register VPNs are **all interconnected dots pointing towards one large goal: the erosion of privacy and the ability to track all citizens.**"

We must consider the use of national intelligence services and military spy agencies in relation to a larger trend in global pandemic responses: the securitization of national health. Around the world, military and security forces were given extraordinary powers to enforce curfews and lockdowns, resulting in excessive use of force in at least 18 countries, where military and police forces "physically assaulted journalists, bloggers, and protesters, including some who criticized government responses to Covid-19", according to a 2021 Human Rights Watch report. Reports from our research partners returned cases of excessive and lethal use of force by military personnel while enforcing quarantine, resulting in hospitalizations in Indonesia and deaths in South Africa and Kenya. These incidents demonstrate the need for government accountability and proportionality in enforcement during a public health crisis. Though these instances of violence do not appear to be directly linked to any particular surveillance technologies or measures, they highlight the **grave consequences that can result when extraordinary powers are deployed without safeguards**. They also demonstrate states' willingness to use force against people during a national health emergency, a disturbing precedent that could be **intensified when coupled with powerful surveillance technologies**.

Professor Fionnuala Ní Aoláin, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, has commented on the folly of relying upon the security sector to manage complex public health needs. Counter-terrorism frameworks are notorious for sidestepping human rights, for unlawfully targeting civil society groups, ethnic, religious and other minorities, for lack of transparency and for covert or unaccountable practices. These same concerns apply when counter-terrorism laws and technologies are repurposed for new objectives. In the examples given above, we have seen how governments have stretched the interpretation of "national security" to include the pandemic response and have used counter-terrorism laws and technologies to infringe upon people's privacy, as well as freedoms of expression, movement and assembly.

In sum, our primary concerns related to the repurposing of existing security measures for surveillance purposes are:

1. The increased surveillance and censorship of civil society through the repurposing of counter-terrorism legislation;
2. The deployment of military and/or counter-terrorism technologies against people, infringing upon their fundamental rights, including the right to privacy; and
3. The excessive use of force against people while carrying out emergency surveillance measures.

Trend 2: Silencing civil society

Freedom of expression and opinion are issues that took on new importance during the pandemic, as governments sought to limit the spread of misinformation and disinformation about Covid-19. While there are legitimate public safety concerns about false information, **some governments used the pretext of combating misinformation as a justification to censor expression and suppress critique.**

The chilling effect of criminal penalties

Under Trend 1, we discussed how some governments invoked cybercrime laws to restrict speech. Other countries pursued similar outcomes through different legal strategies. For example, Russia made legislative changes to its Criminal Code that "introduced criminal penalties for 'public dissemination of knowingly false information' in the context of emergencies, and administrative penalties for media outlets that publish such information", while the Philippines passed a law declaring a state of emergency, including a provision that penalized the spread of "false information". The South African government legislated and criminalized misinformation through the Regulations to the Disaster Management Act of 2002, which gave the government the legal basis to penalize anyone who published any statement through any medium, including social media, with the intention to deceive any other person about Covid-19, the Covid-19 infection status of any person or any measure taken by the government to address Covid-19. Violators faced disproportionate penalties, including imprisonment for up to six months. Such extreme and disproportionate penalties can impact civil society, especially when these penalties are used as a pretext for suppressing critique about government policies. This tactic was used against activists in Cambodia, Iran, India and Thailand, according to human rights observers and media reports.

In Argentina, "cyber patrols" monitored social media activity in order to determine the "social mood" about the pandemic, which authorities claimed was critical for preventing riots. Anyone found guilty of "public intimidation" could be sentenced to up to six years in prison. By the end of the first month of mandatory lockdown, at least 12 people had been accused of "public intimidation" through the spread of misinformation which, according to the head of the Cybercrime Specialized Prosecutor's Unit, could "lead to inciting collective violence".

In Argentina and elsewhere, there was little transparency about the criteria used to define "misinformation" or "fake news", or whether such criteria even existed. Such **lack of transparency leads to arbitrary enforcement and makes it difficult for people accused of spreading misinformation to defend themselves.** The vagueness and ambiguity around terms like "public intimidation" can lead to situations like the case of Kevin Guerra, a 20-year-old Argentinian man who became the subject of a criminal investigation after posting a sarcastic comment to Twitter when he had not yet received his expected welfare benefit payment. **Criminal penalties such as these can have a chilling effect on speech**, limiting people's willingness to express themselves, even in a satirical manner.

Public spaces under surveillance

Another major trend we observed was **the use of surveillance technology to monitor public spaces** under the justification of enforcing lockdown quarantine and social distancing requirements. For instance, in Tunisia a remotely operated robot patrolled the streets, requiring passers-by to show their identification papers to a camera, while police deployed drones in Australia, France, Greece and India. Furthermore, in Kenya and Moldova, governments used CCTV footage and facial recognition technology to monitor public spaces and enforce social distancing requirements. The use of surveillance technologies in public spaces was and continues to be deeply intrusive, especially when coupled with facial recognition capabilities. People moving through public spaces are often unaware of or unable to consent to the capture of their image; furthermore, they are rarely able to obtain information about how their images are being stored or by whom they are being used.

The use of surveillance technology to patrol public space must be considered within a larger context in which peaceful protests were being closely monitored and forcibly dispersed – in some cases violently – under the pretext of enforcing social distancing regulations. For instance, protestors in Kenya were arrested for failing to adhere to Covid-19 rules against public gatherings. Local human rights observers, however, considered these arrests politically motivated, since social distancing rules were unevenly enforced and politicians were able to hold campaign events that gathered crowds, even though the general elections were not scheduled for another 18 months. In Poland, leaders of October 2020 mass protests against a near-total abortion ban are being prosecuted for "causing epidemiological threat". Especially when applied by governments who have a history of quashing dissent, the use of surveillance technologies in public spaces can have a **chilling effect on freedoms of expression, assembly and association**.

In sum, our primary concerns related to the silencing of civil society are:

1. The use of intrusive surveillance technologies in public spaces, having a chilling effect on freedoms of expression, assembly and movement; and
2. The criminal penalties, introduced under the pretext of stopping misinformation, used against civil society.

HIGHLIGHT FROM FRANCE

Illegal drone surveillance

Report by La Quadrature du Net

Starting with the first lockdown, the police began using drones to monitor the population. These surveillance drones had already been owned by the police for many years, but their use was marginal and had not received much media coverage. These drones circulated in the streets of medium and large French cities, depending on the local police equipment. They were often equipped with speakers telling people who were filmed to return to their homes (even though leaving was not forbidden, with many exceptions allowed).

In May 2020, La Quadrature du Net (LQDN) challenged the use of drones in Paris, where the press had been able to gather some technical information that could be used to characterize the existence of illegal data processing before a judge. LQDN won the case before the Conseil d'État, which found that the drones used were processing personal data without any legal basis.

While most local police forces stopped using surveillance drones in May 2020 after LQDN's victory, the police in Paris persevered. With lockdown nearly over, surveillance of demonstrations was documented between May 2020 and October 2020. In October 2020, LQDN again challenged the Paris police over their use of surveillance drones for protest-surveillance purposes. The use of drones was again declared unlawful in December 2020.

Trend 3: Risk of abuse of personal data

As a response to Covid-19, governments around the world introduced various surveillance technologies – such as contact-tracing apps, digital vaccine certificates, electronic wristbands, SIM card tracking and biometric identification – to control the spread of the virus. In many countries, however, state agencies' lack of transparency and accountability about the collection and use of personal data raises serious concerns about **the legitimacy of interference with the right to privacy and the impact that overbroad data collection might have on civic space actors.** Many countries did not have data-protection laws in place, and those that did used exemptions and exceptions to bypass them. Without clarity on the legal basis and purposes of data collection, and without safeguards and oversight mechanisms to prevent the abuse of data, there is a legitimate concern that digital surveillance tools adopted in the name of tackling the spread of the virus may be used to target activists or limit the exercise of civic freedoms.

Lack of clarity around the purposes of Covid-19 apps and applicable safeguards

Many governments introduced mobile contact-tracing apps that collect location data about users through Bluetooth or cellular signals. In 2021, security analysts found that contact-tracing apps were operational in more than 90 countries around the world. Mobile apps were also used to track symptoms and show proof of vaccination or recovery in order to access indoor spaces or be allowed to travel. These applications were rolled out without a prior assessment of the legal framework regulating them, their effectiveness or whether appropriate safeguards were in place. The data collected by these apps varied. Some apps paired location tracking with a biometric check-in component, such as in Australia or Poland, where people who had been diagnosed as positive with Covid-19 were made to participate in random facial recognition check-ins to ensure they were complying with quarantine rules. As a whole, **Covid-19 apps were rapidly developed and introduced.** Many users reported software glitches and false alarms. Moreover, the case studies conducted by local civil society organizations participating in this report relayed that their

governments did not properly communicate about how contact-tracing apps functioned, what information they collected or how this information was analysed, used, stored and shared.

Rule of law concerns

A related issue is **overbroad data collection that was disproportionate to the stated objective of curbing the spread of Covid-19 and, in some cases, lacked a legal basis (as detailed later in this report).** For example, in India, the framework governing the use of the contact-tracing app was entirely made up of **delegated, instead of primary, legislation**, while in France the court held that the government was processing data collected through surveillance drones **without a valid legal basis** (as detailed earlier in this report). When coupled with the overall lack of transparency and accountability around data collection, some users worried that their data could be repurposed for alternative objectives or stored indefinitely in a way that could cause future harm.

Erroneous predictions and few avenues for redress

In some cases, data collected by mobile apps was **used to make predictions about individuals' health through automated processing, including machine learning**. Additionally, some states used algorithmic decision-making systems to determine who should receive vaccines or which individuals were eligible for emergency relief benefits. For instance, PanaBIOS, an app employed in Ghanaian border enforcement and backed by the African Union, claimed to use "algorithms to track and trace persons facing potential health threats and track and keep records of test samples from their origin to in-country labs". It was not clear to its users how it collected and shared data. Beyond the typical transparency and accountability concerns associated with contact-tracing apps, there is an extra element of uncertainty when user data is processed by predictive analytics or risk-assessment tools. This is because **users are rarely given information about how automated determinations are made**

HIGHLIGHT FROM INDONESIA

Poor data-storage practices fail to protect users' personal data

Report by KontraS

In order to tackle the Covid-19 outbreak, the Indonesian Ministry of Health built the PeduliLindungi application, which was launched in early July 2021. The PeduliLindungi application was used to monitor people's locations, as well as to provide information to the Indonesian people regarding Covid-19 red zones in various parts of Indonesia, information related to mandatory vaccinations and certificates, Covid-19 test results and certifications needed to be able to access public services.

Another feature of this application was the Electronic Health Alert Card (eHAC). eHAC's specific function was for the Indonesian Ministry of Health to collect data about people who wanted to travel domestically or internationally. It should be noted that eHAC was made mandatory for any person intending to travel, especially those crossing regional or state borders, as well as for foreigners entering the country.

When entering the application, the users were required to provide personal data including their name, residence number (NIK), address, photograph, phone number and email address, without any data-protection safeguards in place.

Unfortunately, the collected data was not kept secure. In August 2021, researchers Noam Rotem and Ran Locar revealed a security vulnerability that exposed the entire infrastructure around eHAC and "left the data of over 1 million people exposed on an open server", including the personal data of Indonesian officials and private hospital records. The researchers also found personal data, ranging from national identity numbers and telephone numbers to Covid-19 test results and location information.

The eHAC data leak confirms that the government failed to ensure that every user is safe in exercising their digital rights. This was not the first time that government data has been leaked. Previously, the government had also failed to guarantee the security of national health insurance and election data. Poor system management and inadequate security infrastructure are the main causes, as well as the lack of data-protection laws.

and have few avenues for redress. In July 2022, travellers reported that the ArriveCAN app, which is required to cross the Canadian border, was incorrectly notifying them to quarantine. A spokesperson from the Canada Border Services Agency confirmed that they had "identified a technical glitch with the app" that "can produce an erroneous notification instructing people to quarantine". The case of the ArriveCAN app demonstrates the lack of accountability around these apps – and the disruptive effects that false predictions can have on people's lives. When apps produce false positives, this can result in confusion and mistrust in public authorities, as was the case in September 2020, after an Irish school had to close to more than half its students when more than 30 of its teachers received false close contact alerts via the Irish contract-tracing app.

In sum, our primary concerns related to the risk of abuse of personal data are:

1. The vast collection of personal data, including sensitive data, without justification or legal basis, which is disproportionate to the stated objective, creating a serious threat of data abuses, including the risk of targeting activists;
2. The lack of transparency and accountability in the collection, use and sharing of personal data, leading to concerns about the repurposing of technology and the use of data for commercial gain; and
3. The lack of transparency around predictive systems based on machine learning and automated processing, with no access to redress.

HIGHLIGHT FROM COLOMBIA

Lack of transparency around contact-tracing app

Report by Dejusticia

In March 2020, a few days after the World Health Organization declared the Covid-19 pandemic, the Colombian government released a mobile app named CoronApp. In doing so, it followed the example set by South Korea and Singapore – the first countries to deploy surveillance technologies to control the spread of the virus. In the Colombian case, however, it was not new technology. In fact, the government renamed an open-source app that has existed since 2017. The app was originally designed to monitor public health in Colombia during Pope Francis's visit.

At first, CoronApp's main objective was to allow people to stay updated on the progression of the pandemic in Colombia. In the days that followed, however, the narrative around the app changed. Its purpose became more ambitious. It soon became a digital tool to keep the population informed and "save as many lives as possible".

This new narrative supported the rapid introduction of new functionalities to the app that, in theory, would allow the government to achieve its grand aims. The original feature – providing reliable information on the pandemic – was supplemented with others: a digital contact-tracing system, a questionnaire to self-report Covid-19-related symptoms and a digital mobility passport.

Contact tracing was implemented with no transparency around what data the app had access to or what smartphone functionalities were needed for it to run. However, the technical analyses carried out by local civil society organizations determined that CoronApp had access to GPS, Bluetooth and Wi-Fi data from the devices it was installed on. Even though the government had access to CoronApp's data from March 2020, users were only informed about that situation in April. The government also failed to reveal which public entities had access to information collected by CoronApp and how gathering this information was useful to control the spread of the virus. There was no transparency about how data was stored or for how long.

Storing massive amounts of data without clear purpose has a stand-alone negative impact on privacy and other civil liberties. Nonetheless, in Dejusticia's view, it is very likely that the government used personal data collected during the pandemic to serve the commercial interests of public companies as they needed to continue their operation. According to public documents released in the course of strategic litigations pursued by civil society organizations, a lot of unannounced third parties had access to CoronApp's database, including: companies from the oil and gas sector, the Administrative Department of the Presidency and the phone company of Bogotá. Users were not made aware of this practice.

Trend 4: The influential role of private companies

Private companies played an important role in many national responses to Covid-19, through data-sharing agreements and/or the development of contact-tracing and digital passport apps. In the early days of the pandemic, governments called upon private companies, such as telecommunications operators and taxi services, to share users' location data. Some laws compelling companies to share telecommunications data with state agencies were struck down by constitutional courts or data protection authorities, for example in Slovakia, Bulgaria, Germany and Slovenia. Data sharing between public and private entities went both ways; for example, in the United Kingdom, the government shared sensitive patient data with companies to process and analyse.

Opaque public-private collaborations

Data-processing and other relationships between governments and private companies were often murky. In some countries, the public was given little or conflicting information about the scope of these partnerships, raising questions about which parties were responsible for holding the data and for how long, what happens to the data after the partnership ends and whether users can be sure that their data will not be misused for marketing or profit-driven activities. Another concern is that people's sensitive data could be used to train machine-learning algorithms and produce software that will be owned by companies. Without sufficient transparency about the agreements made between governments and private companies, it is difficult to know who should be held accountable in the event of data breaches. Furthermore, when governments outsource data-processing and storage tasks, "citizens lose much of their power to hold governments accountable: the government abdicates and transfers responsibility to private actors against which citizens have fewer rights".

Influence of the private sector in setting global standards amid crises

One of the most impactful interventions from the private sector was the Google/Apple Exposure Notification (GAEN) application programming interface (API), a framework upon which contact-tracing apps could be built. The Bluetooth-based GAEN API, which was used in nearly 40 countries, served as a basic building block to help enable local, regional and national governments to build their own contact-tracing apps. The API was immensely popular as governments were under pressure to quickly produce mobile apps for contact tracing, particularly because it guaranteed seamless compatibility with mobile devices using Google and Apple operating systems – respectively, Android and iOS. As Marcel Salathé, a digital epidemiologist who worked on developing the SwissCovid app, explained, "You want to have a tool that works on users' phones, and Google and Apple control 99.5% of operating systems." Countries who sought to build their own applications were stymied by the fact that Google and Apple operating systems restrict background Bluetooth broadcasting, which would **lower the efficacy of any app developed without cooperation with the tech giants**. This is likely why both Germany and the UK abandoned their independently developed apps to switch over to the GAEN API system. The popularity of the GAEN API raises **significant concerns about the power of private corporations to determine responses to the pandemic and set global standards amid a public health crisis**. The enormous influence of Google and Apple and their ability to impose contact-tracing standards on governments around the world introduces serious questions about democratic oversight and accountability.

Furthermore, researchers have questioned whether the GAEN API sufficiently protects users' privacy. One study found that for Android phone users, the Irish GAEN contact-tracing app necessitated the turning on of Google Play Services and therefore sent data to Google servers every 20 minutes, while the same group of researchers

discovered that Google periodically received "serial numbers of SIM cards and hardware, phone IMEI, MAC address, and user email address with Google, along with fine-grained information about other apps running on the phone". Other complaints include the potential for cyberattacks and false positive alerts that provide incorrect information about Covid-19 exposure. When one considers the questionable accuracy of the contact-tracing apps powered by the GAEN API, data leakage becomes more concerning, as users may have put their personal data at risk in exchange for an app that does not even meet its stated purpose of reducing Covid-19 exposure. An issue of transparency also arises, with the authors of the Android/GAEN study noting the problematic discrepancy between the Irish health authority's component of the app receiving considerable public scrutiny, including a Data Protection Impact Assessment, and the lack of public documentation on the GAEN component of the same app. They concluded "given that many governments are encouraging entire populations to use these apps it is necessary that the detail of their operation be visible to enable properly informed choices by users and potential users of these apps".

In sum, our primary concerns related to the role of private companies are:

1. Unlawful access to telecommunications and other corporate data by state agencies;
2. The lack of transparency about data-processing agreements between the public and private sectors, as well as applicable safeguards, leading to possible data abuses;
3. The lack of public scrutiny of private-sector tools as part of state responses, leading to the use of data by private companies for their own interests; and
4. The assertion of state responsibilities, allowing private companies to set global standards amid a public health crisis, posing potential risks for democratic oversight and accountability.

HIGHLIGHT FROM SOUTH AFRICA

Privacy concerns around over-reliance on WhatsApp

Report by the Legal Resources Centre

The primary technologies which the South African government introduced to control the spread of Covid-19 were the COVID Connect app, which was launched in July 2020, and the COVID Alert SA app, which was launched in September 2020 as South Africa's official contact-tracing and exposure-notification app. COVID Connect began as a WhatsApp channel to provide accurate information about Covid-19. Over the next few months, COVID Connect expanded to become a service that provided healthcare information, screening and contact-tracing processes. COVID Alert SA was launched as an app which would work alongside COVID Connect. The COVID Alert SA app was built on the (GAEN) API and worked via Bluetooth by sending exposure notifications to users who had been in close contact with another user who had tested positive for Covid-19.

Technical reviewers commissioned by the public interest group ALT Advisory examined both of South Africa's Covid-19 apps and raised concerns about the reliance on WhatsApp as a communications platform. The technical reviewers explained that the use of WhatsApp's API to notify COVID Alert SA users of the results of their Covid-19 tests raises privacy concerns, regardless of how convenient it may be. This approach potentially allows a third party with commercial interests to identify which users have been diagnosed as Covid-19 positive. This is not required by the GAEN framework and therefore appears to have been a choice made by the developers. Although the content of the messages is encrypted, one can anticipate that assumptions – such as a person's Covid-19 status – may be drawn when a user of the app engages the National Department of Health via WhatsApp.

Trend 5: Normalization of surveillance beyond the pandemic

The majority of Covid-19 surveillance measures were introduced during the first year of the pandemic. At the time of writing this report in the second half of November 2022, we can observe how some of these extraordinary measures have been extended, or how data collected under the pretext of fighting Covid-19 has been used for other purposes. Our major concern is that **the pandemic has provided an entry point for invasive government surveillance to become normalized even after the threat from the virus has receded.**

We must consider the repurposing of Covid-19 infrastructure in relation to **a larger tendency towards overbroad government surveillance after national emergencies**, under the logic that security can only be achieved by accumulating more and more information. The most notable example of this tendency is the expansion of governments' surveillance powers after the 9/11 terrorist attacks in the US, which established a worldwide infrastructure of invasive data collection still present 20 years later, despite reports of little to no counter-terrorism benefit.

Repurposing of Covid-19 apps

In Guatemala, for example, the government provided an app called Alerta Guate to disseminate public health information. While the original stated purpose of the app was to provide information about Covid-19, in March 2020 President Alejandro Giammattei stated that it "will also have other functions" and that people should continue using the app after the pandemic subsides to receive information about "security issues" and to aid the search for missing children. Giammattei's comments reveal that even in the early days after releasing the app, the presidency was already imagining alternative uses for the technology. The expanding purpose of the Alerta Guate app is **a prime example of mission creep**, a term that describes when a measure or tool originally designed for one specific purpose is later reused to serve other objectives. Furthermore, privacy advocates expressed concern that the Alerta Guate app "asks permission to access files, calls, and audio" and collects user information, including location data, social media handles and "personal interests", which is retained for ten years. Overbroad data collection and storage, when combined with a tendency towards mission creep, are especially concerning in the Guatemalan context – that of a country in which the government has historically carried out high-tech surveillance against "politicians, journalists, diplomats and social leaders" and where attacks against human rights defenders reached historic levels in 2020. For this reason, the then Guatemalan Ombudsman for Human Rights, Jordán Rodas Andrade, lambasted the Alerta Guate app, calling it "extremely risky for the health of democracy and civil liberties".

National governments in Colombia, India and Kenya have announced similar plans to **continue using apps introduced during the pandemic for non-emergency purposes**. After its national health emergency was suspended in July 2022, the Colombian government rebranded its CoronApp as MinSalud Digital and transferred responsibility from the National Digital Agency to the Ministry of Health; along with this transfer of responsibility came the transfer of data to the new authority. Separately, in March 2022, the South African government declared its intention to expand the Electronic Vaccination Data System (EVDS) and "use it as a potential springboard to launch a portable healthcare record system". These moves raise privacy and data-protection concerns as people who initially registered for a vaccine through EVDS or used CoronApp for contact tracing would have been unaware that their personal data could be linked to a larger national healthcare information system.

The transfer of personal data from a platform intended for the narrow objective of tracking Covid-19 outbreaks to a different system that has a broader mandate around general national health is likely to **violate the principle of purpose limitation.** Data-protection laws in many countries require that data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, especially when people did not have a choice on whether or not to provide their data.

Abuse of data collected for emergency health purposes

We have also observed that **some governments have accessed data that was collected under the justification of public health and used it for alternative non-health-related purposes.** In Australia, for example, Privacy Commissioner Angelene Falk found evidence that the police had accessed check-in histories from Covid-19 mobile apps without a judicial warrant to do so in order to assist them in their investigations. In Hungary, government officials took email addresses which were used to register for Covid-19 vaccines and used them for direct political marketing in support of incumbent Prime Minister Viktor Orbán right before the 2022 general elections. In both cases, data that was collected for the purposes of managing the Covid-19 pandemic was exploited without user awareness or consent, in the case of Australia infringing criminal procedure rules as well as the privacy of Australian citizens and residents, and in the case of Hungary, using data improperly to try to influence the election in favour of the incumbent government.

In sum, our primary concerns related to the normalization of surveillance are:

1. The indefinite, unspecified or opaque repurposing of surveillance technologies originally introduced to fight the spread of the pandemic; and
2. The use of data collected under the pretext of fighting the spread of the pandemic for non-emergency, non-health-related and illegitimate purposes.

HIGHLIGHT FROM INDIA

Controversies around the new purpose of the contact-tracing app and its impact on the right to privacy

Report by Amber Sinha

In July 2022, it was announced that the government intends to convert the Aarogya Setu contact-tracing app into a "national health app", and not an app only intended as a response to the Covid-19 pandemic. Shockingly, the government also discontinued the app's data-access and knowledge-sharing protocol, which raised serious questions among privacy advocates about how the data would be used. The discontinued protocol had previously set limitations around how Aarogya Setu could handle and share people's personal data; without the protocol, there were concerns about how the app would handle data going forward, especially as the app's purpose was also expanding.

There was no notification of this discontinuance provided to users, and it came to light only in response to a freedom of information application filed by the Internet Freedom Foundation under India's Right to Information Act. The Internet Freedom Foundation also sought information regarding the fate of data collected during the pandemic; however, the government did not give a clear answer on whether this data had been deleted, as originally announced. This confirmed the earlier-stated fears of privacy activists that the app would be used for purposes other than those related to general national health services.

There continues to be uncertainty about the state of data collected by the app. When the Internet Freedom Foundation sent a follow-up Right to Information request seeking answers on whether the data collected had been deleted, the response by the government simply redirected them to the app's privacy policy. The privacy policy states that "Deleting the app will delete all the information collected and stored on your phone but will not delete any information stored on the cloud. If you wish to delete the registration information referred to in Clause 1(a) and stored on the backend servers, you may cancel your registration." This contradicted newspaper reports quoting an unnamed government official's statement that all data had been purged from the app and government servers.

Successful civil society actions to challenge surveillance measures

Throughout the pandemic, civil society organizations have played an important role as watchdogs. We are indebted to the work that these organizations have done to monitor the ongoing crisis and document the impacts of Covid-19 surveillance measures on human rights and fundamental freedoms. Here, we provide a few examples of strategic litigation campaigns led by civil society to resist unlawful surveillance in and of their communities. This list is by no means exhaustive; our intent is to share these success stories to provide useful frameworks for organizations in other jurisdictions.

The fight against drones in France

In the pandemic's early days, France entered a national lockdown and police in 15 jurisdictions employed hundreds of drones to monitor and enforce stay-at-home orders. The police drones were equipped with cameras and speakers that made announcements telling people to return to their homes. In May 2020, LQDN and La Ligue des Droits de l'Homme filed a lawsuit to block the use of drones to enforce Covid-19 lockdown in Paris. Their cases hinged on data-processing and -retention rules: **they argued that the police did not have a legal basis to process people's personal data when recording them via drones.**

The Conseil d'État, the highest administrative court in France, found the Paris police to be in violation of the Computer and Freedoms Act of 6 January 1978, which protects individual liberties in the course of processing personal data. The decision issued by the Conseil d'État made it illegal for the police to fly drones equipped with cameras at a low enough altitude that individuals could be identified from their clothing or other distinctive signs. Exceptions would only be granted following a ministerial decree reviewed by the French data protection authority (CNIL). Though this case was raised because of surveillance conducted during the Covid-19 pandemic, its impact was broader, since the March 2020 Conseil d'État ruling also blocks police use of drones for other investigative purposes.

Successful civil society actions to challenge surveillance measures

LQDN's victory, however, was marked by ongoing challenges. Between May and October 2020, the Paris police continued to use drones, including to surveil political demonstrations. They claimed that this usage was lawful because they used an AI-powered tool to blur the drone footage, though media reports found the images could "easily be 'unblurred'". LQDN filed another complaint against the Paris police in October 2020, arguing that drone surveillance infringed upon civil liberties and freedom of expression. They were successful once again and the Conseil d'État decreed that the Paris police must "cease, with immediate effect, carrying out surveillance measures by drones of public gatherings of people". This decision has even more wide-ranging implications than the ruling from May 2020 because it concludes that police usage of drones is a substantive and not just a procedural matter. LQDN reports that this decision severely undermines the French government's ability to authorize the use of drones through Article 22 of the new Global Security Law, since they will now need to prove that drones are an absolute necessity to ensure public safety.

This victory underlined the need for clear and explicit legal bases for such surveillance tools. LQDN has published the full text of their legal claims on its website, allowing groups to reuse this argumentation for other cases. For instance, in March 2022 a group inspired by LQDN raised a complaint with the administrative court of Lyon and successfully banned surveillance helicopters used by the police.

Defending fundamental freedoms in Colombia

As we detailed under Trend 3, the government of Colombia issued a contact-tracing app, CoronApp, that received considerable criticism from politicians and members of civil society for its lack of transparency and accountability. While public officials claimed that the app was voluntary, watchdogs reported instances where its use became quasi-mandatory; in November 2020, a group of Colombian women – Claudia Julieta Duque, Juanita Goebertus, Sol Marina de la Rosa and Alejandra Martínez – were repeatedly told by airport authorities that they must download the app to their phones in order to board their flights. One of the women, Claudia Julieta Duque, refused and was not allowed on the plane. Duque is a journalist who has previously been subjected to persecution by the state and was therefore especially concerned that her privacy might be compromised.

Following the airport incident, the women filed a writ of protection of constitutional rights against the Ministry of Health, the National Institute of Health and the Airport Regulations Agency, requesting the Constitutional Court to intervene and protect the plaintiffs' rights to privacy, data protection and freedom of movement. The women argued that their fundamental rights were violated when they were forced to download CoronApp in order to travel and requested the Court to order public authorities not to make the app mandatory. In particular, they invoked protection of "individuals' right to know, update and rectify information gathered about them in databases or files".

The women also received support from civil society groups, such as AccessNow and Dejusticia, who both filed amicus briefs with the Constitutional Court. AccessNow emphasized the importance of free and informed consent and the provision of alternatives so that people could access key services without using the app. Dejusticia questioned whether the app was truly voluntary, since thousands of passengers were compelled to download it in order to enter or leave the country.

For more than a year the women's litigation was pending, and during that time the app ceased to be mandatory. Ultimately, in April 2022 the Constitutional Court reviewed the case and determined that their rights were no longer at risk of being violated since the app was no longer mandatory. However, in analysing the merits of the case, the Court determined that the plaintiffs' rights to privacy should be respected, even during a national state of emergency. Furthermore, they declared that authorities had a duty to "avoid the abusive and arbitrary use of personal data" and the National Data Authority was ordered to erase the plaintiffs' data. The writ of protection raised by Duque, Goebertus, de la Rosa and Martínez and subsequent decision by the Constitutional Court will therefore have important implications for future public health crises and national states of emergency.

Successful civil society actions to challenge surveillance measures

Resisting mass surveillance in Israel

As we described under Trend 1, the Israeli national intelligence service Shin Bet was given expanded powers during the pandemic, granting it the authority to retrace the movements of people who had been diagnosed with Covid-19 and those who might have been infected due to proximity. These measures were introduced as emergency regulations by the executive branch and were not subject to parliamentary oversight.

On March 18, 2020, the day after the emergency measures were announced, attorneys from the Association for Civil Rights in Israel (ACRI) submitted a petition to the High Court of Justice, arguing that the executive branch should not be able to bypass parliament and authorize mass surveillance. On April 26, the High Court found that Shin Bet was "not constitutionally authorized to collect, process and use 'technological information'" of Covid-19 patients. The Court ruled that without passing legislation, the government did not have the authority to grant power to Shin Bet to surveil people under the pretext of combating the spread of Covid-19.

In July 2020, parliament passed legislation to temporarily authorize Shin Bet to use mass surveillance tools to track Covid-19 infections for a period of six months. In response, a coalition of Israeli human rights defence groups in Israel – ACRI, the Adalah Center, Physicians for Human Rights Israel and Privacy Israel – filed another petition to the High Court in September 2020 calling to repeal the law. In the petition, they asserted that Shin Bet's mass surveillance program was not proportional to the goal of fighting Covid-19 since it infringed upon fundamental freedoms and the right to privacy. Furthermore, they argued that the recently passed law was unconstitutional, since it allowed a national security tool to be used for civilian purposes. In January 2021, the High Court ultimately ruled that "broad surveillance severely violates human rights" and ordered the government to cease broad use of the Shin Bet tracking tool, stipulating that in the future the tool could only be used in cases where people refuse to cooperate with epidemiological investigations.

Over the course of a year, ACRI submitted half a dozen petitions to the High Court, some of which were rejected and had to be resubmitted. Eventually, their tenacity paid off. With each petition, ACRI included additional arguments to further bolster its case. Initially it challenged the legality and constitutionality of emergency measures that bypassed parliament, while later arguments were introduced on the basis of privacy, proportionality and effectiveness.

Conclusion

The rapid introduction and repurposing of surveillance measures and technologies to fight the Covid-19 pandemic has had downstream impacts on human rights, fundamental freedoms and the rule of law. Around the world, governments developed and deployed tools – in many cases with little public oversight – that violate people's right to privacy and threaten their civic freedoms. Nearly three years after the start of the pandemic, it seems that governments, international organizations and individuals have moved on, accepting the surveillance measures and practices we have seen. But these measures and practices should not be normalized considering the effect on our freedoms and democracies. Now is the time to take stock, assess the efficacy and proportionality of the surveillance measures and technologies introduced to fight the pandemic, and determine what lessons have been learned so that governments and civil society are better prepared for the next global emergency.

Our research allowed us to identify five overarching trends in Covid-19 surveillance:

1. Repurposing of existing security measures

Counter-terrorism architecture and surveillance tools operated by national intelligence services were transferred to the civilian purpose of pandemic response. For more than a decade, human rights defenders have documented how counter-terrorism laws operate with little transparency and accountability and have been used to quash dissent and silence critique. These same concerns apply when counter-terrorism frameworks are applied in pandemic response. For instance, we found evidence that cybercrime laws were expanded to censor critical voices and persecute people accused of spreading misinformation about the pandemic in **Bangladesh, Indonesia, Kenya, Niger and Saudi Arabia.** The ease with which counter-terrorism frameworks were repurposed demonstrates that when the definition of "terrorism" is vague, it can be instrumentalized by states for repressive measures.

Right to freedom of expression

Under the justification of combating misinformation about Covid-19, governments repurposed cybercrime laws, introduced new legislation that penalized the spread of "fake news" and monitored social media activity. However, in countries including **Cambodia, Iran, India** and **Thailand**, this resulted in increased surveillance and censorship of journalists and members of civil society, who faced criminal penalties or had their content removed when they were accused of spreading misinformation.

Conclusion

2. Silencing civil society

With a similar motivation to repurposed cybercrime laws, countries including **the Philippines, Russia** and **South Africa** introduced new legislation to criminalize pandemic-related misinformation. When combined with disproportionate penalties – up to six years of jail time in **Argentina** – and unclear criteria to define what qualifies as misinformation, these measures contribute to a climate of fear and intimidation, particularly in countries where activists and journalists have historically been targeted. Furthermore, states introduced technologies like drones, patrol robots and facial recognition under the justification of enforcing mandatory lockdowns, thereby increasing the surveillance of public spaces and posing a threat to freedom of assembly. It is difficult to measure the full impact of Covid-19 surveillance measures on civic space: rarely will someone definitively state that they did not attend a demonstration or express their opinion on social media because they feared surveillance and reprisal. However, given the larger context in which public assemblies were banned and protestors forcibly dispersed in at least ten countries worldwide, we can conclude that the "chilling effect" of surveillance technologies significantly contributes to the silencing of civil society.

Right to freedom of assembly

Surveillance technologies – such as drones, patrolling robots and facial recognition – were deployed to monitor public spaces in the name of enforcing quarantines and lockdowns. However, these technologies can also produce a chilling effect on people's willingness to gather in public and express their political opinions, especially when coupled with other phenomena observed during the pandemic, such as the banning of protests and large gatherings, uneven enforcement of social distancing rules and excessive force against people who contravened lockdown orders.

3. Risk of abuse of personal data

Governments introduced various tools designed to trace the spread of the virus – many of which depended upon the collection of personal data. These technologies were rapidly designed and introduced with little public consultation or oversight. We determined that many contact-tracing apps did not meet fundamental data-protection principles like legality, necessity, proportionality and data minimization. For instance, the Constitutional Court of **Colombia** eventually determined that data collection connected to the mandatory use of the country's contact-tracing app was unlawful. In **Australia** and **Hungary**, we found evidence of government officials using Covid-19 patient data for police investigations and direct political marketing – a clear abuse of data that had originally been obtained for a narrow purpose. Overall, the local civil society organizations who conducted case studies observed a lack of transparency and accountability around Covid-19 tracing apps. Such opacity makes it difficult to assess whether data collection was proportional to apps' intrusiveness and whether the same public health aims might have been achieved by way of other means, or by way of alternative non-rights-violating measures.

Right to privacy

In many countries, the pandemic response relied upon the vast collection of personal data, including sensitive data, without clear justification or demonstration of its proportionality. Sweeping data collection infringed upon the right to privacy, particularly in countries where mass surveillance technology originally designed for counter-terrorism was deployed against citizens, such as **Israel** and **Pakistan**. Intrusive and open-ended data collection poses particular concern for activists and dissidents in countries with poor human rights records.

Conclusion

4. Influential role of private companies

Furthermore, we have observed the influential role that private have companies played in the pandemic by cooperating with governments to develop contact-tracing apps and tools and engaging in data-sharing agreements. In countries like **Colombia** and the **United Kingdom**, governments entered opaque public–private partnership agreements, the entire scopes of which were only revealed after activists demanded transparency through freedom of information laws. This lack of transparency makes it difficult for civil society to understand the extent of data sharing between governments and private companies, evaluate the risk of data abuse, and determine who to hold accountable in the case of data breaches, as occurred in **Indonesia**. As one of the first major global health events of the smartphone era, the Covid-19 pandemic has also exposed the growing influence of tech giants like Google and Apple. Because these companies control the operating systems of mobile devices, private enterprise is able to dictate the protocols for contact-tracing apps and shape public health responses, raising important questions about the proper role of private companies and democratic oversight and accountability.

Right to freedom of movement

The use of location-tracking tools – such as contact-tracing apps, electronic wristbands and data gleaned from telecommunications companies – allowed governments to trace people's locations, movements and associations. Without these surveillance tools, governments would have been less able to enforce exceptional measures that imposed mandatory lockdowns and quarantines that infringed upon people's freedom of movement and restricted their ability to travel within national borders.

5. Normalization of surveillance beyond the pandemic

Towards the end of 2022, some governments began to phase out the surveillance tools and measures introduced during the pandemic, such as the government of Canada, which announced its plan to decommission its Covid-19 contact-tracing app in June 2022. We applaud these efforts. However, in other places, we have observed the continuation and normalization of state surveillance. In this report, we have described how states repurposed counter-terrorism laws and technologies and applied them to civilians in the name of fighting Covid-19. Now, we must be wary of the opposite phenomenon: the normalization and repurposing of Covid-19 measures and tools. We have good reason to fear the possibility of mission creep, as we have already seen some governments announce their intentions to use data collected during the pandemic for secondary purposes, such as the development of national health platforms in **Colombia, India,** and **South Africa**. On the surface, this shift from Covid-19 to general public health may appear unproblematic. However, the use of data originally collected in exceptional circumstances for non-emergency purposes violates the principle of purpose limitation and contributes to the normalization of a surveillance state that accumulates large amounts of data about people in a way that is disproportionate to its necessity and intrusiveness.

Recommendations

Summary

Based on the findings, we have developed detailed recommendations for states, companies and civil society. These recommendations reflect discussions with the broader community of civic actors, including participants in a workshop organized during the Internet Governance Forum 2022 in Addis Ababa, Ethiopia.

Our recommendations to states focus on the need to conduct a serious review of surveillance technologies used during the Covid-19 pandemic and to draw lessons from this experience for future crises. First, states should remedy the hasty and opaque development of surveillance tools and engage in a careful assessment of their human rights impacts. Measures that do not comply with human rights standards and/or are no longer necessary for the pandemic response should be ceased. Second, as our partners on the ground often struggled to obtain even basic information, such as the legal basis or the current status of a surveillance measure, we see an urgent need for states to commit to transparency measures including the routine publishing of laws, regulations, guidance and policies. In the detailed recommendations below, we outline the minimum amount of information that should be made public. Third, states should examine laws and policies introduced or applicable during the pandemic and assess their compliance with international human rights standards. This process should be conducted in public and in dialogue with relevant stakeholders, including civil society, and should lead to the development of clear human rights safeguards for the use of surveillance tools in future emergencies. These safeguards, which are themselves consistent with international human rights law, should be translated into relevant laws and processes. We specify key elements of these frameworks below, including data-protection safeguards and sunset clauses to prevent repurposing of emergency measures.

Considering **the influential role of private companies in designing and deploying technological responses to the pandemic,** we see an urgent need for improvement in terms of transparency about these partnerships with state agencies and also about companies' own practices, especially when it comes to data protection. We call on companies to review their technologies from the perspective of human rights and to cease developing and selling those that do not comply with international standards, including data-protection laws. Companies should also put in place human rights policies and procedures guiding the development of technology for future emergencies and how they plan to respond to government requests to access data.

Finally, we see an **important role for civil society** in monitoring states' responses to emergencies and private companies' practices, and assessing them through the lens of human rights. As demonstrated by the examples of successful litigation and advocacy that we highlight in this report, civic pressure is necessary to promote public debate about surveillance technologies and measures and to keep states and private companies accountable.

Detailed recommendations

For state actors

Review of surveillance measures and laws

- **Review** all surveillance measures, technologies and systems deployed to address the Covid-19 pandemic to assess their compatibility with and impact on human rights, including data-protection legal frameworks;
- Following the assessment, **cease** surveillance technologies and measures that are incompatible with international human rights standards and applicable laws;
- **Delete** personal data and **deactivate** applications that are no longer necessary;
- Publicly review the compatibility of **states' domestic laws and policies** that were applied during the pandemic with international human rights law and data-protection regimes; and
- **Provide remedies** for any and all identified human rights violations.

Recommendations

Transparency about surveillance measures during the Covid-19 pandemic

Make public, at minimum:

- All surveillance measures, technologies and systems used since the beginning of the pandemic and whether they are still in use and why;
- Technical specifications of any applications, systems and devices deployed during the pandemic, regardless of whether they have been phased out;
- All public–private partnerships, including agreements and relevant documentation, entered into since the beginning of the pandemic, as well as the existing partnerships that were drawn upon during the pandemic;
- Results of any reviews conducted, including human rights impact assessments and reviews of efficacy and how they informed decision-making; and
- Data-processing records, including data protection impact assessments, information on the kinds of data collected and for what purposes, which parties had access, how long it will be stored or whether it was deleted, and how data subjects' rights were guaranteed.

Safeguards for the use of surveillance measures in future emergencies

- **Revise** and/or develop legal frameworks and procedures regulating surveillance measures and technologies, as well as the role of the private sector, to ensure they are compliant with international human rights standards.

  Any laws and policies regulating surveillance powers in the context of emergencies should require state agencies to:
  - ◊ Conduct and publish human rights impact assessments, including data protection impact assessments, for each surveillance measure or technology.
  - ◊ Provide evidence that a specific measure or technology is compliant with human rights standards. Define a periodic review process to assess its efficacy and compliance.
  - ◊ Implement data-protection safeguards, including at minimum: a clear and appropriate legal basis; a limited and specific purpose for processing personal data and limiting the processing only to the data which is necessary for this purpose; clearly defined data-retention periods and a "sunset clause" for all measures or technologies; and respect for people's rights, including access to information and remedies.
  - ◊ Establish appropriate and effective oversight mechanisms.
  - ◊ Refrain from repurposing adopted measures and tools.

- Ensure **meaningful public participation and consultation** in the process of designing, developing, deploying, updating and reviewing adopted surveillance measures or technologies. In particular, establish oversight committees involving all relevant stakeholders, including technologists, civil society, academia and members of communities most affected by adopted measures to regularly review adopted tools.
- Ensure that surveillance measures, tools and laws including those adopted in the case of emergencies are **not used to stifle dissent or civic participation.**
- Ensure that surveillance measures, tools and laws do not result in people's movements, behaviours and/or health statuses being used for profit and/or commercial interests.
- Ban general and indiscriminate biometric surveillance in public spaces.

Recommendations

For companies

- Review technologies and systems deployed during the Covid-19 pandemic to ensure they **comply with international human rights standards,** including the UN Guiding Principles on Business and Human Rights, and national laws.
- **Cease** any activities that cause adverse human rights impacts or take necessary steps to mitigate those impacts.
- **Adopt human rights policies** that apply to the company's activities, including procedures for assessing government requests to access data in a manner which, to the extent possible, ensures compliance with international human rights standards.
- Publish, and make directly available to people affected, information about **data-processing activities,** measures put in place to protect personal data and existing grievance mechanisms.
- **Publish transparency reports** outlining the instances when user data has been requested and shared with state agencies, the types of user data (including metadata) requested and shared, the overall number of requests and the rate of compliance.
- Make publicly available information about entering into a **public–private partnership** with the state agency, including at minimum the nature and the purposes of the partnership, its duration, information about processing personal data and the rights of people affected.
- Ensure access to appropriate **remedies** when the company's actions have caused or contributed to adverse impacts.

For civil society

- **Monitor and investigate** governments' Covid-19 surveillance measures and their level of compliance with international human rights standards as well as local and regional laws, in particular data-protection laws. If appropriate, **pursue communications and legal avenues** to challenge these measures.
- Remain watchful about the possibility of **mission creep** and urge governments to introduce and respect **sunset clauses** that commit to deleting data and dismantling surveillance systems as soon as they cease to be strictly necessary.
- **Demand transparency from state agencies about:**
  - ◊ Long-term plans for data collected as part of the Covid-19 response to gain clarity about data usage, storage and repurposing;
  - ◊ Data-sharing agreements between state agencies, including supra-national bodies;
  - ◊ Data-sharing agreements between the public and private sectors;
  - ◊ Demonstrable evidence of efficacy of surveillance tools and measures; and
  - ◊ Regular reviews of how communities most or disproportionately affected by surveillance tools and measures are being affected.
- Advocate for the review or development of appropriate legislation and policies for future health crises and other emergencies, and demand that civil society is consulted in this process.
- **Apply pressure to companies** to hold them accountable for adverse human rights impacts caused by their activities.

About us

This report is a joint effort by the European Center for Not-for-Profit Law, members of the International Network of Civil Liberties Organizations and Privacy International, with research and editing support from Nina Dewi Toft Djanegara.

The **European Center for Not-for-Profit Law Stichting (ECNL)** staff has over 20 years of experience in building and advocating for better legal and policy environments for civic groups, movements and activists. It creates knowledge and works with partners to set global and regional standards to protect and expand civic freedoms online and offline. It focuses on global drivers that affect these freedoms and the complex needs of civil society, including the need to streamline fundamental rights safeguards in the development and functioning of technology and artificial intelligence (AI) systems and devices. When it comes to addressing the impact of technology on civic space, ECNL builds bridges between policy makers, academics and industry on the one hand and non-digital-rights civil society organizations, including representatives of marginalized and vulnerable groups, on the other. It has (co-)established civil society thematic networks (e.g., on monitoring protests, counter-terrorism and AI) and developed monitoring tools on civic space (e.g., Covid-19 Civic Freedom Tracker). It also engages in advocacy related to global, regional and national laws and policies related to AI and emerging technologies, including the EU AI Act and the Council of Europe Framework Convention on AI. ECNL is a member of the Global Internet Forum to Counter Terrorism and the Financial Action Task Force Private Sector Consultative Forum, an affiliate of the European Digital Rights initiative (EDRi) and the representative of the Conference of International Non-Governmental Organisations (CINGO) of the Council of Europe's Committee on Artificial Intelligence.

The **International Network of Civil Liberties Organizations (INCLO)** is a network of 15 independent, national human rights organizations from different countries in the North and South that work together to promote fundamental rights and freedoms. INCLO supports and mutually reinforces the work of member organizations in their respective countries and collaborates on bilateral and multilateral bases. INCLO believes that member organizations are stronger together, able to help deliver lasting victories, amplify each other's success and share knowledge, skills and resources. INCLO has decades of experience winning meaningful social change across the globe, drawing upon its deep knowledge of the legal, political and cultural landscapes in 15 countries. INCLO empowers people to own their futures and build the tomorrow we need for everyone to live safely and freely as they are. The findings in this report are generally endorsed by INCLO members Agora, the Association for Civil Rights in Israel, the Canadian Civil Liberties Association, Centro de Estudios Legales y Sociales in Argentina, the Hungarian Civil Liberties Union, the Human Rights Law Centre in Australia, the Irish Council for Civil Liberties and Liberty in the UK.[2]

Privacy International (PI) is a London-based non-profit, non-governmental organization (charity number: 1147471) that works globally with partners to advocate for legal and technological solutions to protect people and their data from exploitation by governments and companies. It exposes harm and abuses, mobilizes allies globally, campaigns with the public for solutions and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how people's personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

Research for the national case studies was conducted by project partners in six countries: Colombia (Dejusticia), France (La Quadrature du Net), India (Amber Sinha), Indonesia (KontraS), Kenya (Kenya Human Rights Commission) and South Africa (Legal Resources Centre). Local partners were given a list of questions to guide their research efforts. The case studies included in this report were written by the partner organizations, with editorial feedback from ECNL, INCLO and PI.

Centro de Estudios de Derecho, Justicia y Sociedad (**Dejusticia**) is a centre for legal and social studies dedicated to strengthening the rule of law and promoting human rights in Colombia and the Global South. It promotes social change through rigorous studies and solid public policy proposals and conducts advocacy campaigns in high-impact forums. It also conducts strategic litigation and design and delivers educational and training programmes.

[2] Although the report doesn't cover the situation in the United States, the American Civil Liberties Union endorses the main recommendations made in the report.

About us

La Quadrature du Net (**LQDN**) promotes and defends fundamental freedoms in the digital world. LQDN fights against censorship and surveillance, both from states and from private companies. It questions how the digital world and society influence each other and works for a free, decentralized and empowering internet.

Amber Sinha is an independent researcher who works at the intersection of law, technology and society, and studies the impact of digital technologies on sociopolitical processes and structures. His research aims to further the discourse on regulatory practices around the internet, technology and society. Until June 2022, he was the Executive Director of the **Centre for Internet and Society, India**,where he led programmes on privacy, data governance, AI and identity. He is currently a Senior Fellow, Trustworthy AI at Mozilla Foundation studying models for algorithmic transparency and Director of Research at Pollicy Data Institute, Kampala. Amber's first book, *The Networked Public*, was released in 2019. He studied law and humanities at National Law School of India University, Bangalore.

KontraS, the Commission for the Disappeared and Victims of Violence, is a national non-governmental human rights organization based in Jakarta, Indonesia. Its main activities are geared towards support for the victims of human rights violations. It seeks to improve respect and protection for human rights within Indonesia through advocacy, investigations, campaigns and lobbying activities. KontraS monitors several issues, such as enforced disappearances, torture, impunity and violations of civil, political, economic, social and cultural rights.

The **Kenya Human Rights Commission** (**KHRC**) is a premier and flagship non-governmental human rights and governance institution that was founded in 1992 with a mission to foster human rights, democratic values, human dignity and social justice. It deals with human rights and social justice issues and situations at all levels of society. The KHRC's interventions are executed under four interdependent strategic objectives and thematic programmes: Civil and Political Rights; Economic and Social Rights; Equality and Non-Discrimination; and Institutional Development and Sustainability. The KHRC is recognized for its long history, tenacity, consistency, expertise and passion for providing technical and political leadership around pertinent human rights and governance programmes at all levels.

The **Legal Resources Centre** (**LRC**) is a public interest, non-profit law clinic in South Africa founded in 1979. The LRC has, since its inception, shown a commitment to work towards a fully democratic society underpinned by respect for the rule of law and constitutional democracy. The LRC uses the law as an instrument for justice to facilitate the vulnerable and marginalized to assert and develop their rights, promote gender and racial equality and oppose all forms of unfair discrimination, as well as to contribute to the development of human rights jurisprudence and the social and economic transformation of society.

Acknowledgements

Nina Dewi Toft Djanegara (Stanford University), Karolina Iwańska, Katerina Hadzi-Miceva Evans, Andrea Judit Tóth, Emily Lawton (ECNL), Olga Cronin, Lucila Santos, Elizabeth Farries, Myriam Selhi (INCLO), Ilia Siatitsa (Privacy International)

Daniel Ospina Celis, Lucia Camacho, Juan Carlos Upegui (Dejusticia), Bastien Le Querrec (La Quadrature du Net), Amber Sinha (Pollicy), Nadine Sherani, Rozy Sodik, Auliya Rayyan (KontraS), Martin Mavenjina (Kenya Human Rights Commission), Sherylle Dass, Devon Turner (Legal Resources Centre)

We also thank Ivana Rosenzweigova for her contribution to the project and Taryn McKay for graphic design.

December 2022

European Center for Not-for-Profit Law

INCLO
INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

PRIVACY INTERNATIONAL