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

Global lessons from the Covid-19 pandemic

In the months following the beginning of the Covid-19 pandemic, more than half the world's countries enacted emergency measures. With these measures came **an increase in executive powers, a suspension of the rule of law, and an upsurge in security protocols** – with subsequent impacts on fundamental human rights. Within this broader context, we have seen **a rapid and unprecedented scaling up of governments' use of technologies to enable widespread surveillance.** 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.

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 deployed during the Covid-19 pandemic on activist movements and organizations**, in collaboration with local organizations and researchers in 6 countries: 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), and Sherylle Dass, Devon Turner (Legal Resources Centre). In the report, we propose recommendations to ensure more human rights-centered technological responses to future emergencies. This report is part of the **Emergency Powers Coalition**, a collective of civil society organizations globally, taking action to resist and roll back emergency powers in national laws and strengthen standards in international fora.

Findings - 5 overarching trends

Trend 1: The repurposing of existing security measures

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. 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. 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.

Trend 2: The silencing of civil society

Countries such as the Philippines, Russia, and South Africa introduced new legislation to criminalize pandemic-related misinformation. When combined with criminal 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. Surveillance technology was also used to monitor public spaces under the justification of enforcing lockdown quarantine and social distancing requirements. Within a larger context in which peaceful protests were being closely monitored and forcibly dispersed – in some cases violently – under the pretext of violating social distancing regulations, the use of surveillance technologies in public space can have a chilling effect on freedoms of expression, assembly, and association, especially when applied by governments who have a history of quashing dissent.

Trend 3: The risk of abuse of personal data

Governments introduced various technological tools designed to trace the spread of the virus — many of which depended upon the vast collection of personal data, including sensitive data. These technologies were rapidly designed and introduced with little public consultation or oversight. We determined that many contact tracing or quarantine enforcement apps were introduced 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. The lack of transparency and accountability in the collection, use and sharing of personal data, as well as the functioning of predictive systems, led to concerns about the repurposing of technology, the use of data for commercial gain and lack of access to redress.

Trend 4: The influential role of private companies

During the pandemic companies cooperated with governments to develop contact-tracing apps and tools and engaged in data-sharing agreements that were often murky. In countries like Colombia and the United Kingdom, the scope of opaque public-private partnership agreements were only revealed after activists demanded transparency through freedom of information laws. The Covid-19 pandemic also exposed the growing influence of tech giants such as Google and Apple who were able to dictate the protocols for contact-tracing apps and as a consequence shape public health responses, raising important questions about democratic oversight and accountability over private companies' ability to set global standards amid crises.

Trend 5: The normalization of surveillance beyond the pandemic

We have good reason to fear the possibility of mission creep, as we have already seen some governments announce their intention to use data collected during the pandemic for secondary purposes, such as the development of national health platforms in Colombia, India, and South Africa. 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:

For state actors:

- Conduct a serious human rights review of surveillance technologies used during the Covid-19 pandemic
- Make public information about surveillance measures, their current status, and compliance with human rights standards
- Create legal safeguards for the use of surveillance measures in future emergencies

For companies:

- Improve transparency about public-private partnerships and data sharing agreements
- Publish, and make directly available to people affected, information about data processing activities
- Assess human rights compliance of technologies deployed during the pandemic
- Adopt human rights policies that apply to the company's activities

For civil society:

- Monitor and investigate surveillance measures and their compliance with international human rights standards
- Advocate for the review or development of relevant legislation
- Demand transparency from state agencies and private companies

European Center for Not-for-Profit Law
INCLO INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS
PRIVACY INTERNATIONAL